

CompTIA[®] Linux+[™] Powered by LPI

CompTIA[®] Linux+[™] Powered by LPI

Part Number: NH85099EBEE
Course Edition: 1.01

ACKNOWLEDGMENTS

Project Team

Content Developer: Nagarajan DR • **Content Manager:** Pradeep Reddy • **Graphic Designer:** • **Project Manager:** Abbas A. • **Media Instructional Designer:** Nagarajan DR • **Content Editor:** Carolin S • **Materials Editor:** • **Business Matter Expert:** • **Technical Reviewer:** • **Project Technical Support:** Mike Toscano

NOTICES

DISCLAIMER: While Element K Corporation takes care to ensure the accuracy and quality of these materials, we cannot guarantee their accuracy, and all materials are provided without any warranty whatsoever, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. The name used in the data files for this course is that of a fictitious company. Any resemblance to current or future companies is purely coincidental. We do not believe we have used anyone's name in creating this course, but if we have, please notify us and we will change the name in the next revision of the course. Element K is an independent provider of integrated training solutions for individuals, businesses, educational institutions, and government agencies. Use of screenshots, photographs of another entity's products, or another entity's product name or service in this book is for editorial purposes only. No such use should be construed to imply sponsorship or endorsement of the book by, nor any affiliation of such entity with Element K. This courseware may contain links to sites on the Internet that are owned and operated by third parties (the "External Sites"). Element K is not responsible for the availability of, or the content located on or through, any External Site. Please contact Element K if you have any concerns regarding such links or External Sites.

TRADEMARK NOTICES: Element K and the Element K logo are trademarks of Element K Corporation and its affiliates.

Red Hat Enterprise Linux 5 is a registered trademark of Red Hat Inc., in the U.S. and other countries; the Red Hat products and services discussed or described may be trademarks of Red Hat Inc. All other product names and services used throughout this course may be common law or registered trademarks of their respective proprietors.

Copyright © 2012 © 2012 Logical Operations, Inc. All rights reserved. Screenshots used for illustrative purposes are the property of the software proprietor. This publication, or any part thereof, may not be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, storage in an information retrieval system, or otherwise, without express written permission of Logical Operations, 500 Canal View Boulevard, Rochester, NY 14623, (585) 240-7500, (800) 478-7788. Logical Operation's World Wide Web site is located at www.logicaloperations.com.

This book conveys no rights in the software or other products about which it was written; all use or licensing of such software or other products is the responsibility of the user according to terms and conditions of the owner. Do not make illegal copies of books or software. If you believe that this book, related materials, or any other Logical Operations materials are being reproduced or transmitted without permission, please call (800) 478-7788.

COMP TIA[®] LINUX+[™] POWERED BY LPI

LESSON 1 - FAMILIARIZING YOURSELF WITH LINUX

A. Review the History and Development of Linux	2
Open Source Software	2
The GNU Project	3
Copyleft	4
The Linux Operating System	5
Uses of Linux	6
Benefits of Linux	7
Linux Distributions	7
Software Acquisition	8
B. Enter Shell Commands.	10
The CLI	10
The GUI	10
Shells	11
Virtual Terminals	13
Shell Commands	13
The date Command	15
The cal Command	16
The uptime Command	17
The who Command	18
The whoami Command	19
The hostname Command	19
The w Command	20
The last Command	21
The echo Command	21
The sleep Command	22
The cat Command	23
The which Command	24

CONTENTS

C. Get Help Using Linux	29
Linux Documentation	29
Manual Pages	30
The apropos Command	31
Other Built-In Help Options	32
Online Help	33
D. Start and Stop Linux	39
Services	39
Daemons	40
Init Runlevels	40
The Upstart Init Daemon	41
The Systemd Init Daemon	42
System Booting	42
System Shutdown	42

LESSON 2 - MANAGING USER AND GROUP ACCOUNTS

A. Create User and Group Accounts	48
User Accounts	48
The useradd Command	49
Default User Accounts	50
Passwords	50
The /etc/passwd File	51
Groups	53
The /etc/group File	54
B. Configure User Profiles	58
User Profiles	58
Global User Profiles	59
Skel Directories	59
C. Manage User and Group Accounts	65
The userdel Command	65
The usermod Command	66
Lock User Login	67
Group Management	67

LESSON 3 - MANAGING PARTITIONS AND THE LINUX FILESYSTEM

A. Create Partitions	76
Filesystems	77
Filesystem Labels	77
Filesystem Types	78
Partitions	80
Partition Types	81
The fdisk Utility	81
fdisk Utility Options	82
The fstab File	83
The mkfs Command	84
The mke2fs Utility	85
Device Recognition by the MBR	85
Partition Management	86
The sfdisk Utility	86
The GNU Parted Utility	87
The partprobe Program	88
B. Navigate Through the Linux Filesystem	94
Filesystem Hierarchy	94
The FHS	94
Standard Directories	95
File Naming Conventions	96
File Browsers	96
The Home Directory	97
The Current Working Directory	98
The Parent Directory	99
Paths	99
Absolute and Relative Paths	100
Basic Filesystem Commands	101

CONTENTS

C. Manage the Filesystem.	106
Filesystem Management Tasks	106
Burning Discs	107
Mount Points	107
The mount Command	107
mount Command Options	108
Swap Space	109
The mkswap Command	110
Swap Partition Management Commands	110
D. Maintain the Filesystem.	116
Filesystem Maintenance Tasks	116
Storage Devices	116
Journaling Filesystems	117
The fsck Command	117
The tune2fs Utility	118
The dumpe2fs Utility	119
The debugfs Utility	120
xfs Tools	120

LESSON 4 - MANAGING FILES IN LINUX

A. Create and Edit Files	130
Text Editors.	131
List of Text Editors.	132
The vim Command	132
Vim Modes	133
Switch Modes	133
Execute Mode Commands	134
Vim Help Options	134
Motions	135
Editing Operators	136
Counts	136
The diff Command	137
The wc Command	138
The tr Command	139
The uniq Command	139
Input and Output Redirection	140
B. Locate Files	147
The locate Command	147
The whereis Command	148
The GNOME Search Tool	149
The find Command	150
find Command Conditions	152
C. Search Text Using Regular Expressions	157
Regular Expressions	157
D. Apply Filters to Text Streams	161
Filters	161
Text Streams	162
E. Link Files	167
Inodes	167
The ln Command	168
Types of Links	168

CONTENTS

F. Back Up and Restore Files	174
Archiving	174
The cpio Command	175
The dd Command	175
The dump Command	176
The tar Command	176
The gzip Command	177
File Archiving Utilities	178
The unzip Command	178
Guidelines to Determine a Backup Strategy	179
The restore Command	180
G. Manage Databases Using MySQL	186
Databases	186
Relational Databases	187
MySQL	187
The MySQL Configuration File	188
mysqld	189
MySQL Commands	189
Joins	191

LESSON 5 - WORKING WITH LINUX PERMISSIONS AND OWNERSHIP

A. Modify File and Directory Permissions	200
Permissions	200
Permission Levels	202
The chmod Command	202
chmod Command Options	203
chmod Modes	203
B. Modify Default Permissions	209
Default File and Directory Permissions	209
The umask Command	209
C. Modify File and Directory Ownership	213
The chown Command	213

D. Set Advanced Permissions	216
Special Permissions	217
The chattr Command	217
The lsattr Command	218
Sticky Bits	219
The Immutable Flag	219
The ACL	220
Advanced Permission Commands	220

LESSON 6 - PRINTING FILES

A. Configure a Local Printer	226
Printer Software	226
PostScript®	227
Linux Compatible Printers	227
CUPS	228
The Print Process	228
Spooling	229
Print Queues	229
B. Print Files	234
Printer Commands	234
The lpr Command	235
The pr Command	235
pr Command Options	236
C. Manage Print Jobs and Queues	239
The printtool and printconf Commands	239
D. Configure Remote Printing	243
Print Servers	243
Remote Printing	243
Remote Printer Permissions	244
Samba	244

LESSON 7 - MANAGING PACKAGES

A. Manage Packages Using RPM	254
Packages	254
Package Managers	255
Dependencies	256
The RPM Package Manager	257
RPM Commands	258
RPM Components	258
RPM Queries	259
B. Verify Packages	262
RPM Verification	263
C. Upgrade Packages	266
Upgrade/Freshen Packages	266
D. Configure Repositories	269
Repositories	270
Types of Repositories	270
The createrepo Command	270
E. Manage Packages Using YUM	274
The YUM Package Manager	274
YUM Commands	275
F. Manage Packages Using the Debian Package Manager	278
The Debian Archive Package Installation Process	278
DEB Tools	278
Debian Archive Package Management Commands	279
The apt-get Command	279
Alien	280
G. Manage Packages Using Source Files	284
makefile	284
Drivers	286
H. Manage Shared Libraries	289
Shared Libraries	289

LESSON 8 - MANAGING KERNEL SERVICES

A. Explore the Linux Kernel	294
The Kernel	295
The Linux Kernel	295
Kernel Layers	295
Types of Kernels Available in Linux	296
B. Customize Kernel Modules	298
Kernel Modules	298
Kernel Module Managing Utilities	299
The modprobe.conf File	301
Kernel Options	302
Types of Kernel Configuration	302
The /proc/version File	302
The sysctl Command	304
C. Create an initrd Image	307
initrd	307
The initrd Image	308
The mkinitrd Command	308
D. Manage Device Drivers	312
udev	312
Device Drivers	313
Device Nodes	314
Special Devices	315
The mknod Command	315
E. Monitor Hardware Devices	317
Hardware Communication Channels	317
The HAL	318
HAL Utilities	318

F. Monitor Processes and Resources	321
Load Average	321
Kernel State Monitoring Utilities	321
Memory Monitoring Utilities	322
Process Monitoring	324
The GNOME System Monitor	325

LESSON 9 - WORKING WITH THE BASH SHELL AND SHELL SCRIPTS

A. Perform Basic Bash Shell Operations	330
The Bash Shell	330
Bash Shell Functions	331
Wildcards	331
Tab Completion	333
The history Command	333
B. Write a Bash Shell Script	340
Shell Scripts	340
#!/bin/bash	341
The test Command	342
C. Customize the Bash Shell	346
Variables	346
Environment Variables	348
The alias Command	349
HISTFILESIZE	350
SUID Scripts	351
Shell Spawning	351
Search Paths	351

D. Redirect Standard Input and Output	359
Standard Input	359
Standard Output	359
Standard Error	360
Redirectors	360
The Pipe Operator	361
The xargs Command	362
The tee Command	363
Command Substitution	363
E. Use Control Statements in Shell Scripts	367
Control Statements	367
Programming Constructs	368
Functions	368
The if Statement	370
The if...else Statement	370
Looping Statements	370
The for Loop	371
The while Loop	372

LESSON 10 - MANAGING JOBS AND PROCESSES

A. Manage Jobs and Background Processes	380
Processes	381
Foreground Processes	381
Background Processes	382
Multitasking	383
The Jobs Table	383
Job Control Tools	385

CONTENTS

B. Manage Processes Using the Process Table	387
The Process Table	387
The ps Command	388
ps Command Options	389
Child Processes	390
The pstree Command	391
Process Identification Commands	392
Signals	393
kill Commands	393
Process States	395
The top Command	395
The nice Command	396
The renice Command	397
The GNOME System Monitor	397
C. Examine Delayed and Detached Jobs	402
Delayed and Detached Jobs	402
The nohup Command	403
D. Schedule Jobs	406
Cron	406
Cron Jobs	407
The tmpwatch Command	408
The logrotate Command	408
The logwatch Utility	409
System crontab Files	410
The at Command	410
Anacron	412

E. Maintain the System Time	415
The NTP	415
The ntp.conf File	416
UTC	416
Locale Settings	417
Clock Drift	419
System Time	419
The Date/Time Format	420

LESSON 11 - MANAGING SYSTEM SERVICES

A. Configure System Services	428
System Initialization	428
The inittab File	428
The /etc/init.d Directory	429
The chkconfig Command	430
The /etc/sysconfig Directory	431
The system-config-services Command	431
The inetd Command	432
B. Monitor System Logs	435
System Logs	435
Logging Services	435
The Central Network Log Server	436
Automatic Rotation	437
The syslogd Utility	437
The klogd Utility	438
The /etc/syslog.conf File	438
Log File Analysis	439
The lastlog Command	440
The grep Command	440
The tail Command	441
The awk Command	442
The sed Command	444

CONTENTS

C. Configure SELinux	450
Types of Access Controls	450
Security-Enhanced Linux	451
SELinux Modes	452
Security Policies	452

LESSON 12 - CONFIGURING NETWORK SERVICES

A. Connect to a Network	458
Networks	458
Types of Networks	459
Network Protocols	460
Types of Network Protocols	460
IP Addresses	461
Subnet Masks	463
IP Address Classes	463
Broadcast Addresses	464
Ports	465
Port Ranges	467
Network Interfaces	468
Network Interface Cards	468
NIC Characteristics	469
The ifconfig Command	470
The iwconfig Command	471
Subnets	472
LDAP	473
The LDAP Process	474

B. Configure Routes	481
Routers	481
Routing	481
Routing Tables	483
The route Command	483
Gateways	485
The traceroute Command	485
The netstat Command	486
C. Configure Client Network Services	491
DHCP	491
The DHCP Process	493
The DNS	493
Domain Names	494
Zones	495
The Domain Name Resolution Process	496
The dig Utility	496
The host Utility	497
The nslookup Utility	498
Resolver Files	498
The named.conf File	499
DNS Resource Records	499

CONTENTS

D. Manage Remote Network Systems	505
PKC	505
The SSH	505
OpenSSH	506
The ssh-agent Program	508
The sftp Command	509
Tunneling	510
X Forwarding	510
VNC	511
The vncserver Command	512
The vncviewer Command	513
The rdesktop Utility	514
The SNMP	514

LESSON 13 - CONFIGURING BASIC INTERNET SERVICES

A. Configure Email Services	524
Mail Protocols	524
The SMTP	525
POP3	526
IMAP	526
Mail Queues	526
The MTA	527
Types of MTAs	527
The MUA	529
The MDA	529
Mail Forwarding	530
The Electronic Mailing Process	530

B. Control Internet Services	543
The xinetd Daemon	543
Telnet	543
The /etc/xinetd.conf File	544
The /etc/xinetd.d Directory	545
xinetd Access Controls	546
Service and Application Access Controls	546

LESSON 14 - SECURING LINUX

A. Examine the Basics of System Security	552
Keys	552
Authentication	553
Encryption	555
Encryption Solutions	555
Random Number Generation	556
Cryptographic Hashes	556
Symmetric Encryption	557
Asymmetric Encryption	557
Digital Certificate Types	559
Package Integrity	559
RADIUS	560
TCP Wrappers	561
B. Secure User Accounts	565
Environment Files	565
Login Levels	565
The su Command	566
The sudo Command	567
Password Policies	568
The Shadow Password File	569
Memory Usage	569
Ways to Improve User-Level Security	569

CONTENTS

C. Enable Firewall Functionality	575
Firewalls	575
Packet Filtering	576
Proxy Server Implementation	577
The iptables Program	578
The ipchains Program	578
D. Implement Security Auditing	581
E. Describe the Intrusion Detection System	584
Network Monitoring Utilities	584
The IDS	585
Tripwire	585
Snort	587
Portentry	587
Nessus	588

LESSON 15 - MANAGING HARDWARE

A. Identify Common Hardware Components and Resources	592
Hardware Components	592
Hardware Resources	592
Disk Space Tracking	594
B. Configure Removable Hardware	597
Removable Hardware	597
The PC Card	597
The cardmgr Utility	598
The pccardctl Utility	599
The USB	600
The Basic Architecture of the Layer Model of a USB Driver	600
FireWire	601
The Loopback Device	601

C. Configure Disk Quotas	604
Disk Quotas	604
Quota Management Commands	605
Quota Reports	605
The quotacheck Command	605
Quota Reports Generation Commands	606

LESSON 16 - TROUBLESHOOTING LINUX SYSTEMS

A. Troubleshoot System-Based Issues	612
Troubleshooting Strategies	612
The Linux Rescue Environment	613
Rescue Environment Utilities	614
Environment Configuration Problems	615
Single-User Mode	616
Boot Disks	617
Root Disks	618
Zero-Filled Files	618
Kernel Panic	618
B. Troubleshoot Hardware Issues	627
Troubleshooting Tools	627
Hardware Problems	628
C. Troubleshoot Network Connection and Security Issues	634
Network Issues	634
Network Troubleshooting Utilities	634
Symptoms of Network Security Problems	635
System Security Monitoring Tools	635
Network Security Vulnerabilities	636
Honeypot Systems	637
Guidelines for Troubleshooting Network Issues	638

LESSON 17 - INSTALLING LINUX

A. Prepare for Installation	644
Hardware Compatibility	644
Linux Installation Methods	646
The Anaconda Installer	647
Partitioning Utilities	648
The FIPS Program	650
BIOS	650
B. Identify the Phases of the Linux Boot Sequence	656
Boot Loaders	656
Boot Loader Components	656
Types of Boot Loaders	657
GRUB 2	657
The Boot Process	658
Superblocks	659
Sectors	660
MBR	660
C. Configure GRUB	662
GRUB	662
The grub.conf File	663
The menu.lst File	663
GRUB Commands	664
GRUB Menu-Specific Commands	665
D. Install the Operating System	670
E. Perform Post-Installation Tasks	678
The X Windows Configuration	678
Virtual Desktops	679
Documentation	679

LESSON 18 - CONFIGURING THE GUI

A. Implement X.	684
X.Org	684
X Servers	685
X Clients.	686
X Font Servers	686
XOrg Runlevels	687
Remote X Sessions	687
Commands Used in Remote X Sessions	688
X-Stations	688
B. Customize the Display Manager	696
Display Managers	696
The GNOME Desktop Environment	697
The KDE Desktop Environment	697
The switchdesk Command	699
C. Customize the Window Environment.	704
The Window Environment	704
The XTerm	704
D. Enable Accessibility Settings in Linux.	710
Accessibility Options	710
Keyboard Accessibility Options	710
Accessibility Based Themes	711
Orca	711

APPENDIX A - MAPPING COURSE CONTENT TO THE COMPTIA LINUX+ POWERED BY LPI CERTIFICATION EXAM OBJECTIVES

APPENDIX B - COMPTIA LINUX+ POWERED BY LPI: ACRONYMS AND ABBREVIATIONS

APPENDIX C - SYNTAX

LESSON LABS 757

CONTENTS

SOLUTIONS	787
INDEX	805

ABOUT THIS COURSE

The *CompTIA® Linux+™ Powered by LPI* certification course, developed to cover CompTIA Powered by LPI exams LX0–101 and LX0–102, builds on your existing user-level knowledge and experience with the Linux operating system to present fundamental skills and concepts that you will use on the job in any type of Linux career.

The *CompTIA® Linux+™ Powered by LPI* certification course can benefit you in two ways. If your job duties include Linux troubleshooting, installation, or maintenance, or if you are preparing for any type of Linux-related career, it provides the background knowledge and skills you will require to be successful. In addition, it assists you if you are preparing to take the CompTIA® Linux+™ Powered by LPI exams (Exam Codes: LX0–101 and LX0–102), in order to become a CompTIA® Linux+™ Certified Professional.

Course Description

Target Student

This course is intended for entry-level computer support professionals with basic knowledge of computer hardware, software, and operating systems, who wish to increase their knowledge and understanding of Linux concepts and skills to prepare for a career in Linux support or administration, or to prepare for CompTIA® Linux+™ Powered by LPI exams (Exam Codes: LX0–101 and LX0–102). A typical student in the CompTIA® Linux+™ Certification course should have at least 6 to 12 months of Linux experience.

Course Prerequisites

To ensure your success, we recommend you first take the following New Horizons courses or have equivalent knowledge:

- *UNIX and Linux: Fundamentals*
- *UNIX and Linux: Advanced User*

How to Use This Book

As a Learning Guide

This book is divided into lessons and topics, covering a subject or a set of related subjects. In most cases, lessons are arranged in order of increasing proficiency.

The results-oriented topics include relevant and supporting information you need to master the content. Each topic has various types of activities designed to enable you to practice the guidelines and procedures as well as to solidify your understanding of the informational material presented in the course.

At the back of the book, you will find a glossary of the definitions of the terms and concepts used throughout the course. You will also find an index to assist in locating information within the instructional components of the book.

As a Review Tool

Any method of instruction is only as effective as the time and effort you, the student, are willing to invest in it. In addition, some of the information that you learn in class may not be important to you immediately, but it may become important later. For this reason, we encourage you to spend some time reviewing the content of the course after your time in the classroom.

As a Reference

The organization and layout of this book make it an easy-to-use resource for future reference. Taking advantage of the glossary, index, and table of contents, you can use this book as a first source of definitions, background information, and summaries.

Course Objectives

In this course, you will acquire the skills needed to install and support one or more distributions of the Linux operating system and learn information and skills that will be helpful as you prepare for CompTIA® Linux+™ Powered by LPI exams (Exam Codes: LX0-101 and LX0-102).

You will:

- identify basic Linux concepts and perform basic Linux tasks.
- manage user and group accounts.
- manage partitions and the Linux filesystem.
- manage various files in Linux.
- work with Linux permissions and ownership.
- print files.
- manage packages.
- manage kernel services.
- work with the Bash shell.

- manage jobs and processes.
- manage system services.
- configure Linux services to provide users with network connectivity.
- configure basic Internet services.
- implement measures to secure a Linux system.
- manage hardware associated with Linux systems.
- troubleshoot Linux system issues.
- install the Linux operating system.
- configure the GUI.

LESSON 1

Familiarizing Yourself with Linux

Lesson Time

2 hour(s)

In this lesson, you will identify basic Linux concepts and perform basic Linux tasks.

You will:

- Identify the key events in the history and development of Linux.
- Enter basic shell commands.
- Access help in Linux.
- Start and stop Linux.

Introduction

You may have experience using the Linux environment, or you may be ready to learn Linux for the first time. In either case, it is good to have an understanding of how Linux was developed and where it is today. In this lesson, you will identify important elements in the history and development of Linux and perform basic Linux tasks.

When Linux was first available, it was not readily accepted by businesses. But today, it is rapidly gaining acceptance in the corporate world, especially for website hosting. Linux is also increasingly used on desktops as a viable alternative to various versions of Microsoft Windows for businesses and individuals alike. By learning the origin of Linux and familiarizing yourself with its basic functions, you will become a more confident Linux user.

This lesson covers all or part of the following CompTIA Linux+ Powered by LPI certification objectives:

- Topic B:
 - Objective 103.1, Objective 103.5, Objective 104.7, Objective 105.2, Objective 109.3
- Topic C:
 - Objective 103.1
- Topic D:
 - Objective 101.2, Objective 101.3, Objective 106.2, Objective 108.2, Objective 110.2

TOPIC A

Review the History and Development of Linux

Operating systems vary greatly from manufacturer to manufacturer. Even if you know very little about the Linux environment, a basic understanding of its roots will be beneficial to you. In this topic, you will identify key events in the history and development of Linux.

Over the past few years, Linux has rapidly gained ground in the competitive operating system marketplace. For example, Linux is now widely preferred for web servers and Internet systems. Many individuals and organizations have accepted it as a desktop and server alternative because of its high security, low cost, and ease of licensing. By learning about the basics of Linux and its development cycle, you will understand and appreciate its benefits.

Open Source Software

Definition:

Open source software enables users to access its source code and gives them the right to modify it. Open source licensing ensures that free and legal redistribution of the software is possible. Although the software can be modified and improved by individual users, the integrity of the author's code is preserved by ensuring that modifications to the original source code are redistributed only as patches.

Example:

Figure 1-1: *Linux is an open source operating system.*

Need for Open Source

In the early days of computing, many programmers freely shared new software they developed with other users, along with the source code. This community approach enabled knowledgeable users to modify and improve the software. However, with the introduction of restrictive licensing practices by big companies, some operating systems and utility programs could not be legally copied by users, and users no longer had access to the source code making it impossible for users to create their own customized versions of the software. Some programmers, therefore, disliked the concepts of closed source and proprietary software. Richard Stallman, then working at MIT's Artificial Intelligence labs, was one such programmer who wanted to create an alternative, open source software. Some examples of open source software used today are Linux, Perl, PHP, Python, and OpenOffice.

Free Software vs. Open Source Software

Although most of the free software is also open source, the terms are not interchangeable. Open source is a development methodology in which anyone can access the source code, though it is possible to prevent any modification of the code by means of a special licensing agreement. Free software focuses on ethical issues of protecting a user's freedom, where there are no restrictions on how the user runs a program or how frequently the user is allowed to copy and share the program.

The GNU Project

GNU's Not Unix (GNU) is a comprehensive computer operating system composed entirely of free software. The *GNU project* was started by Richard Stallman in 1984, as an initiative to produce a source for free and open software. Stallman wrote much of the GNU software himself, including the GNU C compiler or gcc and the emacs text editor. Later, several programmers worked together to develop more utilities that are compatible with GNU utilities.



Richard Stallman chose the recursive acronym "GNU's Not Unix" to show that though GNU was like the free version of *Unix* in its design, it did not contain any code from Unix. Note that the "G" in GNU is included in the pronunciation of the term "guh-NOO."

FSF

The Free Software Foundation (FSF) is a nonprofit organization founded by Richard Stallman in 1984 to promote the development of free software. It advocates the movement against the monopoly of copyrighted, proprietary software by ensuring the availability of all software to users without any restrictions on use, distribution, or modification.

Free software refers to users' rights rather than cost, and so free software may be sold at a price. Free software must not be confused with freeware, which is software that is available free of cost. Freeware may sometimes include even proprietary software offered on a demo basis. For an online source, see <http://www.fsf.org>.

Copyleft

Definition:

Copyleft is the method of ensuring that all original works, and their derivative works, are kept free and open. The term “copyleft” is used to define a concept that is essentially the opposite of “copyright.” Richard Stallman proposed this concept to create a licensing arrangement under which software can be freely used, modified, and copied by others. The Free Software Foundation (FSF) recommends that all free software be copylefted and released under General Public License (GPL).

Example: GNU Utilities

GNU utilities released under GPL are copylefted because they cannot be copyrighted by anyone who modifies them.



Figure 1-2: *The copyleft symbol.*

GPL

GPL is a licensing agreement that effectively enforces public ownership of software released under it. GPL states that a programmer holds the copyright to a specific piece of software. This prevents the software from being placed in the public domain, where anyone can modify it and then copyright the modified version. The software is then subjected to a licensing agreement that allows it to be freely used, modified, and copied. Anyone who modifies the code and distributes it to others must provide the open source code that includes their modifications, making it freely available under the terms of GPL. Copyleft is a principle or standard of which GPL is an implementation. Three versions of GPL are available.

Version	Date of Release
GPLv1	January 1989
GPLv2	June 1991
GPLv3	June 2007

The Linux Operating System

The *Linux* operating system is a complete, open source operating system that combines GNU utilities and the Linux *kernel*. The kernel is the central core of the Linux operating system that manages all the computer's physical devices. The Linux kernel was developed by Linus Torvalds in 1991, while he was a student at the University of Helsinki. A year later, Torvalds released Linux kernel 1.0 under GPL. The Linux commands closely resemble those found in other Unix-type operating systems. Many programs written for other operating systems run on Linux.



Figure 1-3: *Linux is a combination of GNU utilities and the Linux kernel.*

Origin of the Linux Kernel

Linus Torvalds, a student at the University of Helsinki in Finland, independently developed a Unix-like operating system kernel in 1991 for his own use, inspired by another system called Minix. He posted his creation on the Internet and asked other programmers to help him further develop it. At that point, Linux could already run Unix utilities such as bash, gcc, and gnu-sed. Until Torvalds agreed to release Linux under GPL, the GNU project was not a complete operating system and the kernel itself was incomplete as an operating system without utilities.

Linux Timeline

The following table outlines important dates in the development of Linux.

Year	Linux-Related Events
1984	Richard Stallman launched the GNU project.
1989	GNU and GPL were released.
1991	Linus Torvalds developed a Unix-like operating system called Linux (version .02).
1992	Linux kernel 1.0 was released under GPL, and SUSE and TurboLinux were founded.
1993	Red Hat was founded, the Debian project began, and Slackware was first released.
1994	Caldera Inc. was founded.
1995	Red Hat Linux 4.0 was released.
1996	The penguin (Tux) was suggested as the mascot for Linux and Linux kernel 2.0 was released.
1997	Red Hat Linux 5.2 and Debian 1.3 were released.
1998	MandrakeSoft was founded and Debian 2.0 was released.

Year	Linux-Related Events
1999	Red Hat Linux 6.0 and SUSE 6.3 were released.
2000	Red Hat Linux 7.0 and Caldera OpenLinux eDesktop 2.4 were released.
2001	Linux kernel 2.4, SUSE 7.2, Debian 2.23r, Slackware 8.0, Caldera OpenLinux Server, and Workstation 3.1 were released.
2002	GNOME 2.0 was released.
2003	Linux kernel 2.6 and Fedora were released.
2004	The GNU project celebrated its 20th anniversary, and GNOME 2.6 and the first official version of Ubuntu Linux were released.
2005	Red Hat Enterprise Linux 4 was released. Mandrake Linux was renamed as Mandriva Linux.
2007	Red Hat Enterprise Linux 5 and Red Hat Enterprise Linux 5 Update 1 (5.1) were released.
2008	Linux kernel 2.6.28 and Red Hat Enterprise Linux 5 Update 2 (5.2) were released.
2009	Red Hat Enterprise Linux 5 Update 3 (5.3) and Linux kernel 2.6.29 were released. Red Hat Enterprise Linux 5 Update 4 (5.4) and Linux kernel 2.6.30 through 2.6.32 were released.
2010	Red Hat Enterprise Linux 5 Update 5 (5.5) and 2.6.33 were released.

Uses of Linux

Linux is mainly used on servers, workstations, and desktops.

Use	Description
Server	Used as a web server to host websites and as a file server to provide file access for multiple clients. Also used to control and secure network traffic.
Workstation	Designed for a business environment geared toward programmers.
Desktop	Focused on home users who run office and graphics applications and games.

Other Uses of Linux

The Linux operating system is very versatile. It can be used as a:

- Domain name server
- Routing server
- Database server
- Software development platform
- Parallel processor
- Gateway server

Benefits of Linux

Being an open source operating system, Linux is continually evolving with the support of its user base. The benefits of Linux are increasing daily. Some of these include:

- Low cost.
- Easy licensing.
- Increased likelihood of bug detection.
- Better performance and stability.
- Ability to be easily customized.
- Increased security.
- Compatibility of software across different versions.
- And, smaller file sizes and reduced use of system resources.

Drawbacks of Linux

As with any operating system, Linux has some drawbacks. Some of these include:

- Limited number of mainstream applications.
- Possible lack of comfort in believing that a single vendor can provide support.
- The operating system is free, but the cost of teaching employees how to use it can be significant.

Comparing Linux with Other Operating Systems

In many ways, Linux is the same as other operating systems. It has a Graphical User Interface (GUI), and you can use it to edit documents, browse the Internet, and play games. Where Linux stands out is in its stability and reliability. Linux can run on almost all hardware such as Macintosh, PC, and even Mainframe.

Linux Distributions

Since its creation, Linux has evolved into hundreds of distributions, also called distros, each tailored to their designers' needs. If you are a beginner, you will find it easier to choose one of the mainstream distributions depending on the installations. Some common distributions are:

- Red Hat Enterprise Linux
- Fedora
- SUSE Linux Enterprise
- openSUSE
- Debian
- Mandriva
- Ubuntu
- And, Mint

Internet Reference for Common Linux Distributions

You can refer to common Linux distributions in the following Internet sites:

- Red Hat Enterprise Linux—<http://www.redhat.com>
- Fedora—<http://fedoraproject.org>
- Debian—<http://www.debian.org>

- SUSE Linux Enterprise—<http://www.novell.com/linux>
- openSUSE—<http://www.opensuse.org>
- Mandriva—<http://www.mandriva.com>
- Ubuntu—<http://www.ubuntu.com>
- Mint—<http://www.linuxmint.com>

Software Acquisition

There are two ways of obtaining Linux software: purchasing it from a local computer outlet or downloading it from a website. While it is convenient to purchase Linux software from a store, downloading it over a broadband connection is also practical.

Comparing Distributions and Their Packaging Solutions

Linux distributions are similar to each other and each has its own strengths and weaknesses. The software packaged with each distribution can make a huge difference in how Linux works for you. Although you can always download or purchase missing components, the software package is easier to use if the components have already been tested and compiled together to work with your distribution.

ACTIVITY 1-1

Reviewing the Development of Linux

Scenario:

Your manager, Linda, asked you to conduct research on the benefits and disadvantages of utilizing Linux in a business environment. She specifically wants to know about the basic concepts of open source software and compare the features of various Linux distributions.

1. Which of these statements about open source software are true? Select all that apply.
 - a) Its source code is accessible by all.
 - b) Users have the right to modify and redistribute it.
 - c) It is always available at zero price.
 - d) It cannot be updated.
 2. Which of these statements apply to Linux? Select all that apply.
 - a) Increased security
 - b) Proprietary in nature
 - c) Customizable
 - d) Easy licensing procedure
 - e) High cost
-

3. **True or False? Software released under GPL can be modified and copyrighted by any user.**
___ True
___ False
-
4. **What are the advantages of Linux? Select all that apply.**
a) Enables software to be customized.
b) Comes with strong single-vendor support.
c) Increases the likelihood of bugs being detected because of increased numbers of programmers who can view code.
d) Fosters a community among users and a sense of shared responsibility for the software.
-
5. **What are the potential disadvantages of using Linux? Select all that apply.**
a) Licensing Linux is a difficult task and requires large amounts of money.
b) A limited number of mainstream applications is available.
c) Possible lack of comfort in believing that a single vendor can provide support.
d) Mainstream Linux distributions come complete with a set of games and office, network, and graphics applications.
-
6. **True or False? There are a limited number of Linux distributions and that is why users have trouble when deciding which distribution to use.**
___ True
___ False
-
7. **True or False? Because of Linux's simple licensing terms, IT administrators do not have to spend a lot of time monitoring the number of installations or tracking licenses.**
___ True
___ False
-
-

TOPIC B

Enter Shell Commands

Now that you understand the origin of Linux, you should learn its basics so that you can use it. The Linux shell prompt is where you enter commands. In this topic, you will describe the shell and enter shell commands.

Learning to enter shell commands will allow you to interact directly with the Linux operating system. You will be able to utilize Linux commands to perform various tasks. In its formative stages, Linux was operated solely through the command line interface using shell commands. With the addition of the GUI, tasks have become easier, but a lot of power and flexibility still reside in knowing the shell commands.

The CLI

The *Command Line Interface (CLI)* is a text-based interface for the operating system, where a user typically enters commands at the *command prompt* to instruct the computer to perform a specific task. A *command line interpreter*, or command line shell, is a program that implements the commands entered in the text interface. The command line interpreter analyzes the input text provided by the user, interprets the text in the concept given, and then provides the output.

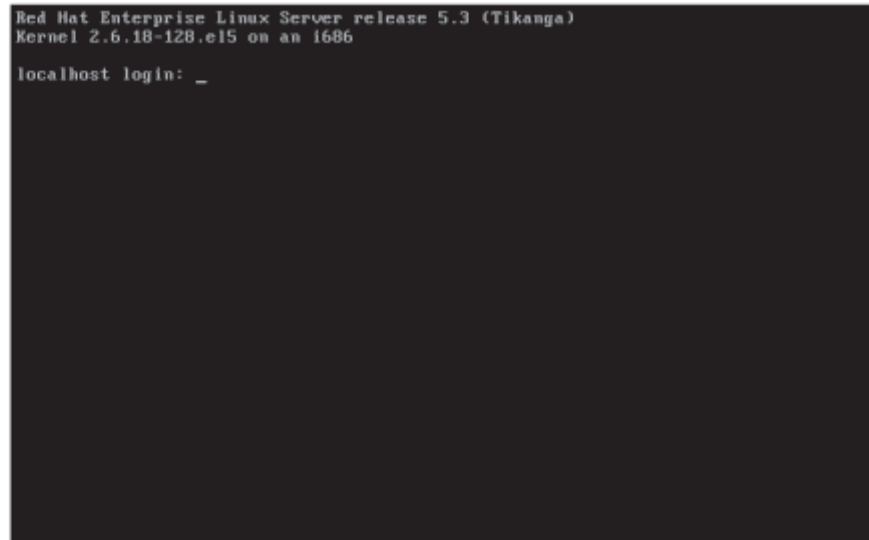


Figure 1-4: A CLI screen.

The GUI

The Linux *Graphical User Interface (GUI)* is a collection of icons, windows, and other screen graphical elements that help users interact with the operating system. The desktop menu provides access to the GUI applications available on the Linux desktop. There are different GUI implementations such as K Desktop Environment (KDE) and GNU Object Model Environment (GNOME).

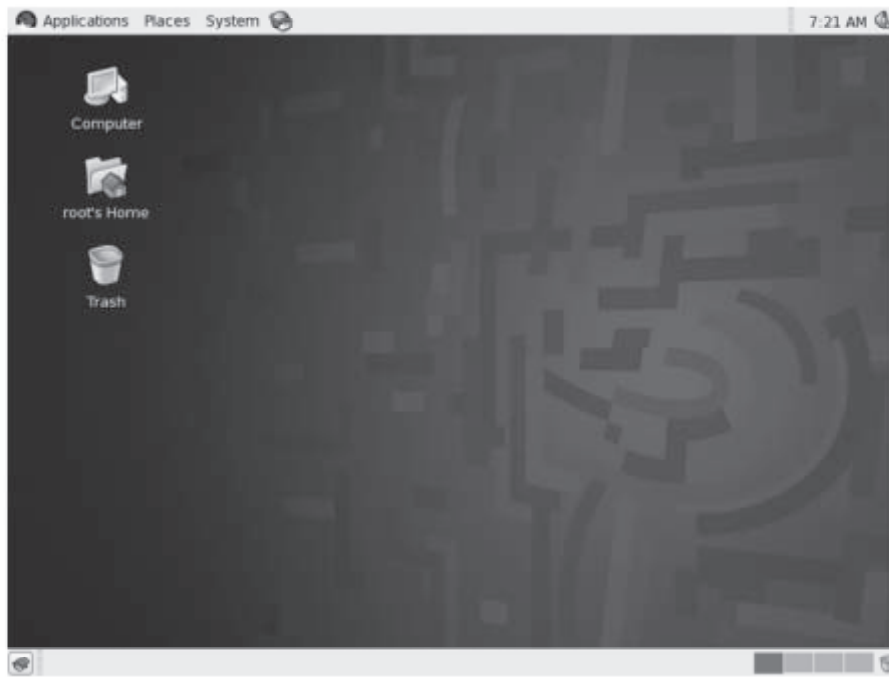







Figure 1-5: A GNOME desktop.

The following table lists the uses of common desktop menu categories in the GNOME GUI.

Desktop Menu Category	Used To
 Accessories	Access applications for performing work-related tasks such as creating text documents and presentations or using a calculator.
 Internet	Access applications for performing tasks on the Internet such as web browsers, email clients, instant messengers, or web editors.
 Sound & Video	Access applications for viewing movies and listening to sound files or CDs.
 System Tools	Access options for changing the settings on the Linux system.
 Help	Access help on Linux.

Shells

Definition:

A *shell* is a component that interacts directly with users. It also functions as the command interpreter for the Linux system. The shell accepts user commands and ensures that the kernel carries them out. The shell also contains an interpretive programming language.

The various shells available in Linux are described in the following table.

Shell	Description
Bash	This is the default Linux shell. It provides the flexibility of the C shell in a Bourne shell-type environment. Use the command <code>bash</code> to open the Bash shell.
Bourne	This is the original Unix shell developed by Steve Bourne at Bell Labs and is available on all Linux systems. Use the command <code>sh</code> to open the Bourne shell.
C shell	This was developed by Bill Joy at Berkeley and was designed to support C language development environments. It was also designed for more interactive use, providing several ways to reduce the amount of typing needed to complete a job. Use the command <code>csh</code> to open the C shell.
Korn	This shell is a combination of the C and Bourne shells. It uses the features of the C shell but the syntax of the Bourne shell. Use the command <code>ksh</code> to open the Korn shell.

Example:



Figure 1-6: A blank shell prompt.



Figure 1-7: The shell prompt in the GUI terminal window.

Opening Multiple Shells

You can have several shells open at the same time with different processes or programs running in each shell. For example, to open a second Bash shell, enter `bash` at the command prompt. To open a C shell, enter `csh`. To close a shell, either enter `exit` or press **Ctrl+D**.

Determining the Current Shell

The `echo` command enables you to determine the shell that is established at the login. To determine the current shell, enter `echo $SHELL`, where `$SHELL` is the environmental variable name that holds the name of the current shell.

View a File One Page at a Time

To view a file one page at a time, simply type the `more` command in front of the file you want to open. For example, if you want to read the `/etc/passwd` file, type `more /etc/passwd`.

The head and tail Commands

The `head` command displays the first 10 lines of each file. The `tail` command displays the last 10 lines of each file. These commands are useful when you only need to see the beginning or the end of a file. For example, you can check recent log entries by viewing the last 10 lines of a log file.

Virtual Terminals

A *terminal* or *console* is a computer interface for text entry and display, where information is displayed as an array of preselected characters. Linux supports six virtual terminals in the CLI mode, which provide a text terminal with a login prompt to the shell. You can choose among these six terminals by using the key combination of **Ctrl+Alt+F1–F6**. You can be logged in to multiple virtual terminals at the same time.

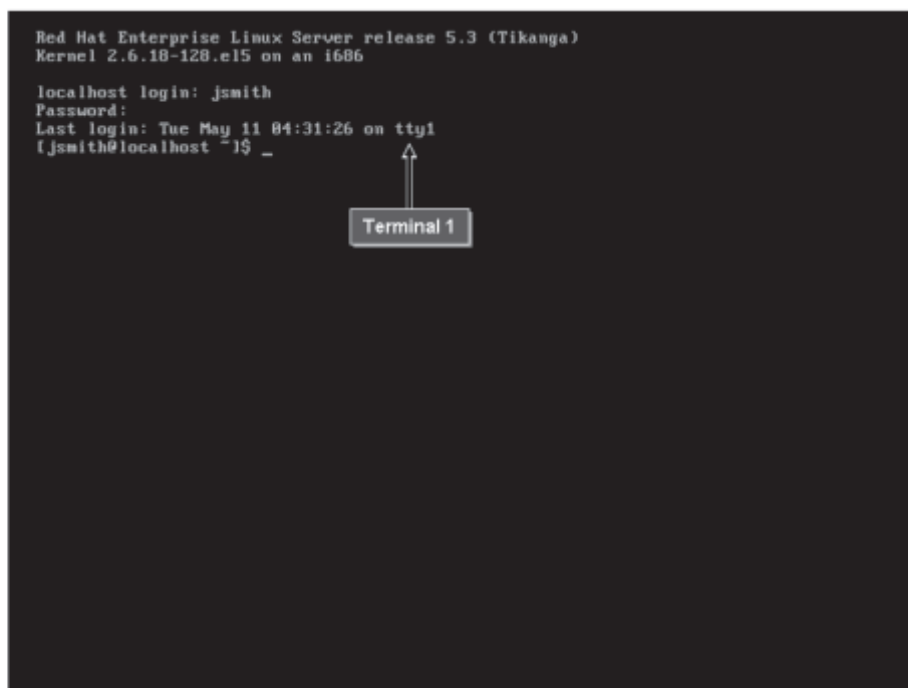
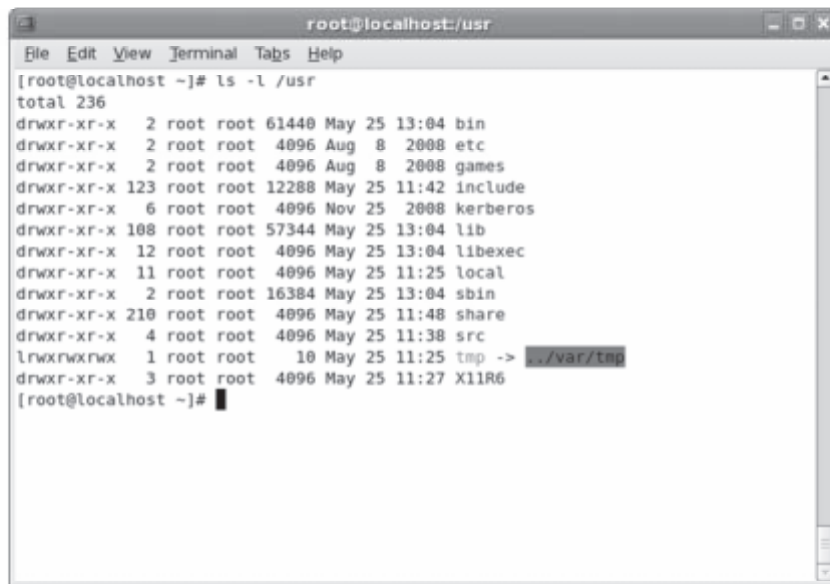


Figure 1-8: Terminal 1 with the user `jsmith` logged in.

Shell Commands

The generic format for a shell command is `command -option argument`. After typing your command, the shell responds by performing a specific action that is associated with that command. Linux is case sensitive, so you must enter commands in the required case.



```
root@localhost:usr
File Edit View Terminal Tabs Help
[root@localhost ~]# ls -l /usr
total 236
drwxr-xr-x  2 root root 61440 May 25 13:04 bin
drwxr-xr-x  2 root root  4096 Aug  8  2008 etc
drwxr-xr-x  2 root root  4096 Aug  8  2008 games
drwxr-xr-x 123 root root 12288 May 25 11:42 include
drwxr-xr-x  6 root root  4096 Nov 25  2008 kerberos
drwxr-xr-x 108 root root 57344 May 25 13:04 lib
drwxr-xr-x 12 root root  4096 May 25 13:04 libexec
drwxr-xr-x 11 root root  4096 May 25 11:25 local
drwxr-xr-x  2 root root 16384 May 25 13:04 sbin
drwxr-xr-x 210 root root  4096 May 25 11:48 share
drwxr-xr-x  4 root root  4096 May 25 11:38 src
lrwxrwxrwx  1 root root    10 May 25 11:25 tmp -> ../var/tmp
drwxr-xr-x  3 root root  4096 May 25 11:27 X11R6
[root@localhost ~]#
```

Figure 1-9: The `ls` command displays the list of files in the `usr` directory.

Argument

An *argument*, also called command line argument, is usually a file name or directory name that indicates the files on which the command will operate. It is used as an input by some commands in Linux. Arguments can be files, directories, commands or even a command switch. For example, `ls {file name}`, `ls {directory name}`, and `ls -l`.

Command History

Sometimes, commands can become quite long. You can access previously entered commands that are stored in the History file by using the **Up Arrow** and the **Down Arrow** keys.

Invoking Commands Outside a Path

There are two ways of invoking a command located outside a path. You can specify the path in which the command is located and then invoke the command. For example, assume that a command is located in the `{user-defined directory}` directory. To invoke this command, you need to enter `{user-defined directory}/{command name}`.

You can also navigate to the directory that contains the command and then invoke it. For example, assume that a command is located in the `{user-defined directory}` directory. You need to change to that directory with the `cd {user-defined directory}` command and then enter `{command name}`.

The Tab-Completion Feature

Some commands have long names containing version number information, weird spellings, or capitalizations. This can make it difficult to correctly enter the commands on the first try. In such a case, you can make use of the tab-completion feature. To use this feature, enter the first few characters of the command and then press **Tab**. If there

is only one match, the rest of the file name is displayed. If you press the next letter of the file name you want and press **Tab** again, the complete file name should come up. If the system still cannot differentiate between the commands, it will beep again, and you have to enter additional characters or press **Tab** two times to view all available options.

Piping Commands

You can send or redirect the results of one command to another command. Pipes are used to combine Linux tools on a single command line, enabling you to use the output of one command as the input to another. The pipe symbol is a vertical bar (|), which you type between two commands. For example, `ls | more` enables you to look at a large directory listing one screen at a time.

Issuing More Than One Command

You can issue more than one command before pressing **Enter**. Place a semicolon (;) between the commands and they will be issued one after the other.

The exec Command

If you enter a command, it runs as a child process to Bash, which is the parent process. If you enter `exec {command}`, the `exec` command will kill the parent process, the bash process, and `{command}` starts to run as the parent process. For example, when a user has a limit applied on the number of process, the user can use the `exec` command to run an additional process by killing the parent process. Once the `exec {command}` is executed, you will be automatically logged out because the bash process has been terminated.

The date Command

The `date` command displays the current date and time set on a system. You can use the hyphen (-) or the colon (:) between the different fields of the date for a clear output.



Figure 1-10: Viewing the current date using the `date` command.

Syntax

The syntax of the `date` command is `date +[format]`, where *format* is the string of characters that are used to display the different fields of the output.

Characters Used with the date Command

The characters that are used to display the different fields of the `date` command are listed below.

Character	Description
%d	Displays the current day of the month (01 to 31).
%D	Displays the date in the format mm/dd/yy, where mm is month, dd is day, and yy is year.
%H	Displays the current hour in the 24-hour format (00 to 23).
%l	Displays the current hour (1 to 12). This option does not display A.M. or P.M. after the hour.
%m	Displays the current month of the year (01 to 12).
%M	Displays the current minute (00 to 59).
%r	Displays the time in the 12-hour format, i.e. hh:mm:ss [A.M. or P.M.].
%R	Displays the time in the 24-hour format, i.e. hh:mm. This option does not display the seconds.
%S	Displays the seconds (00 to 60).
%T	Displays the time in the 24-hour format, i.e. hh:mm:ss. This option displays the seconds also.
%Y	Displays the last two digits of the current year.
%Y	Displays the current year in four digits (yyyy).

The cal Command

The `cal` command displays the calendar for any month or year. If you do not specify the month or year with the `cal` command, it will display the calendar of the current month. You can display the calendar of a specific month in a year by specifying the month and the year after the `cal` command. The year must be specified in the yyyy format. The command `cal 10` will display the calendar for the year 10 A.D. and not for the year 2010.

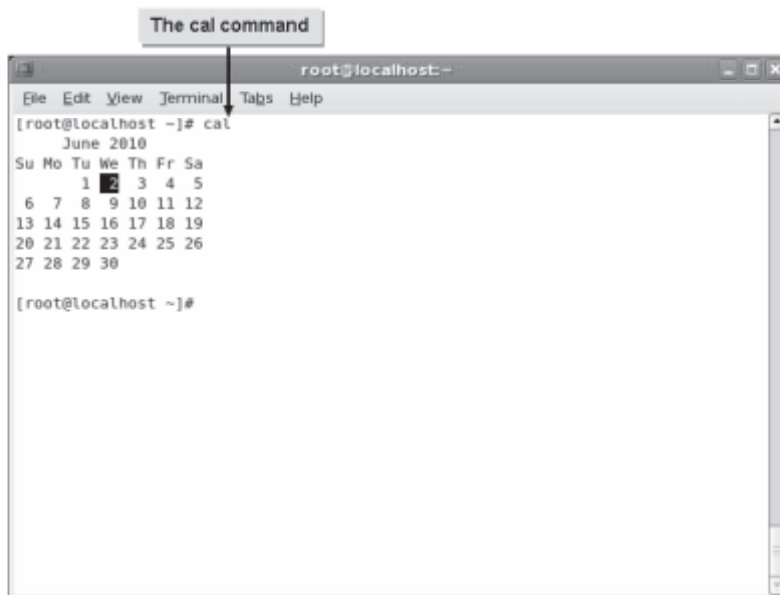


Figure 1-11: Viewing the calendar of the current month using the `cal` command.

Syntax

The syntax of the `cal` command is `cal {month} {year}`.

Options for the `cal` Command

Some options for the `cal` command are listed in the table.

Option	Description
<code>-m</code>	Displays Monday as the first day of the week.
<code>-j</code>	Displays the Julian dates.
<code>-y</code>	Displays the current year's calendar.

The `uptime` Command

The `uptime` command displays the time from when a system started running. The output of the `uptime` command gives information about the current time, how long the system is running, and how many users are currently logged in.

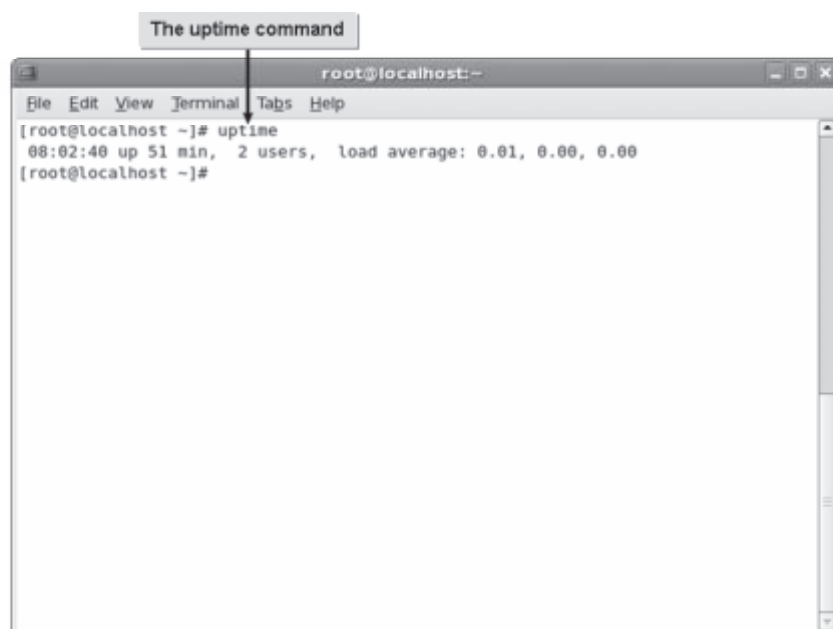


Figure 1-12: Using the uptime command to view the time from when the system started running.

Load Average

The last field of the uptime command output displays the system's load averages for the last 1 minute, 5 minutes, and 15 minutes. This information can be used to check whether the system is busy.

The who Command

The who command is used to determine the details of users currently logged in to a system. The output of the who command includes the user name, the name of the system from which the user is connected, and the time since the user is connected.

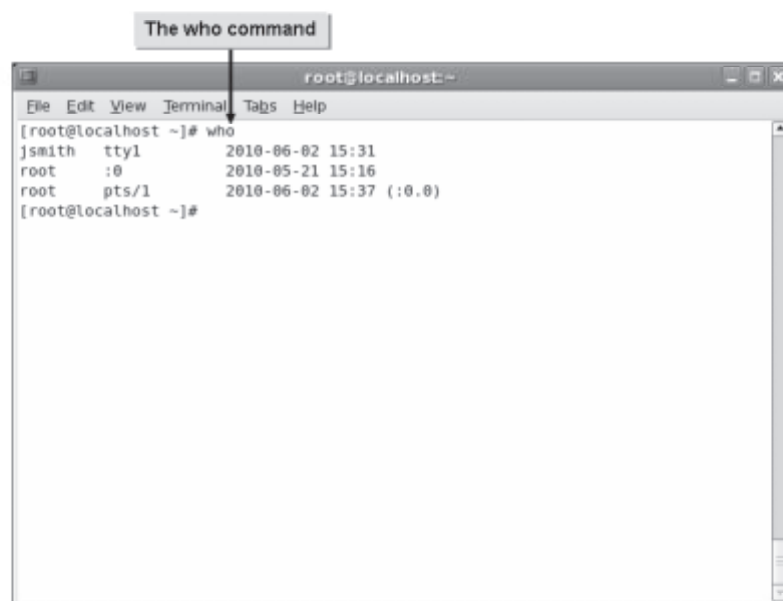


Figure 1-13: Displaying user details using the who command.

who Command Options

The `-i` option can be used to see how long users have been idle. A dot indicates that the users were active up to the last minute, `old` indicates that the users have been inactive for over 24 hours, and anything between 2 minutes and 23 hours 59 minutes shows the length of time they have been idle. The `am i` option displays information only for the user who runs the command. The output is preceded by the hostname.

The whoami Command

The `whoami` command is used to display the user name with which you are currently logged in to the system. Sometimes, you may need to log in to a system and switch among different users, and you may not be sure with which user you are currently logged in. In such instances, you can use the `whoami` command to know your current user name.



Figure 1-14: Displaying the user name using the `whoami` command.

The hostname Command

The `hostname` command is used to display the hostname of the system you are currently logged in to. When you log in to different systems using the same terminal, you can use the `hostname` command to identify the system on which you are presently running the commands.



Figure 1-15: Viewing the hostname of the Linux system using the hostname command.

The w Command

The `w` command is primarily used to display the details of users who are currently logged in to a system and their transactions. The first line of the output displays the status of the system. The second line of the output displays a table with the first column listing the users logged in to the system and the last column indicating the current activities of the users. The remaining columns of the table show different attributes associated with the users.

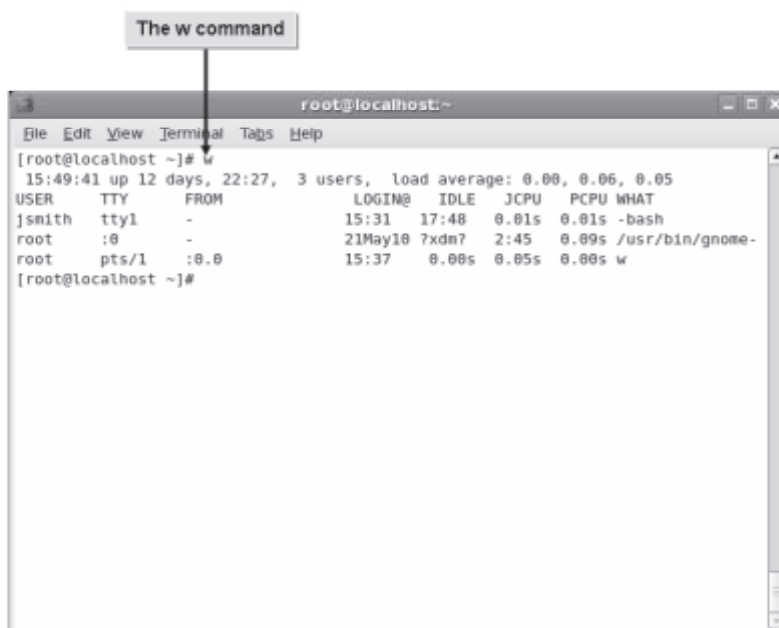


Figure 1-16: Viewing user details using the w command.

The last Command

The `last` command displays the history of user log in and log out, along with the actual time and date. It also has options that enable you to filter users who have logged in through a specific terminal. For example, `last 1` will display the details of users who logged in using the first terminal. The `last` command retrieves information from `/var/log/wtmp` file.

The last command

```

[root@localhost ~]# last
root      pts/1      :0.0          Wed Jun 2 15:37      still logged in
jsmith    tty1       :0.0          Wed Jun 2 15:31      still logged in
root      tty1       :0.0          Tue Jun 1 14:49 - 22:08 (07:19)
root      tty1       :0.0          Tue Jun 1 14:36 - 14:44 (00:07)
root      tty1       :0.0          Wed May 26 16:50 - 14:34 (5+21:44)
root      tty1       :0.0          Thu May 20 18:22 - 16:50 (5+22:28)
root      pts/1      :0.0          Thu May 20 18:21 - 18:21 (00:00)
root      tty1       :0.0          Thu May 20 18:20 - 18:22 (00:02)
root      tty1       :0.0          Thu May 20 17:46 - 18:19 (00:33)
root      tty1       :0.0          Thu May 20 17:46 - 17:46 (00:00)
root      tty1       :0.0          Fri May 21 15:19 - 17:45 (-21:-33)
root      :0         :0.0          Fri May 21 15:16      still logged in
root      :0         :0.0          Fri May 21 15:16 - 15:16 (00:00)
reboot    system boot 2.6.18-128.el5 Fri May 21 14:58      (12+00:51)
root      :0         :0.0          Fri May 21 11:54 - 12:35 (00:41)
root      :0         :0.0          Fri May 21 11:54 - 11:54 (00:00)
reboot    system boot 2.6.18-128.el5 Fri May 21 10:20      (02:15)
root      :0         :0.0          Thu May 20 17:06 - 18:16 (17:10)
root      :0         :0.0          Thu May 20 17:06 - 17:06 (00:00)
root      :0         :0.0          Thu May 20 16:50 - 17:05 (00:15)
root      :0         :0.0          Thu May 20 16:50 - 16:50 (00:00)
root      :0         :0.0          Thu May 20 16:48 - 16:49 (00:01)
root      :0         :0.0          Thu May 20 16:48 - 16:48 (00:00)
  
```

Figure 1-17: Viewing the history details of user logins.

The echo Command

The `echo` command is used to display a line of text on the terminal. It is useful for programmers writing shell scripts because it can be used to display additional information. The text that needs to be displayed should be inserted after the `echo` command. You can also use the `echo` command to display the value stored in a variable by specifying the variable name after the `echo` command.



Figure 1-18: Displaying text using the echo command.

Syntax

The syntax of the echo command is `echo {"string"}`.

The sleep Command


The `sleep` command is used to pause system activities for a specified time. The command `sleep {time}` hangs up the prompt for the number of seconds specified by the value of the variable *time*.



Figure 1-19: Pausing activities using the sleep command.

The cat Command

The `cat` command displays, combines, and creates text files. This command is frequently used to read small text files.

 The name of the `cat` command is a short form of the word concatenate.

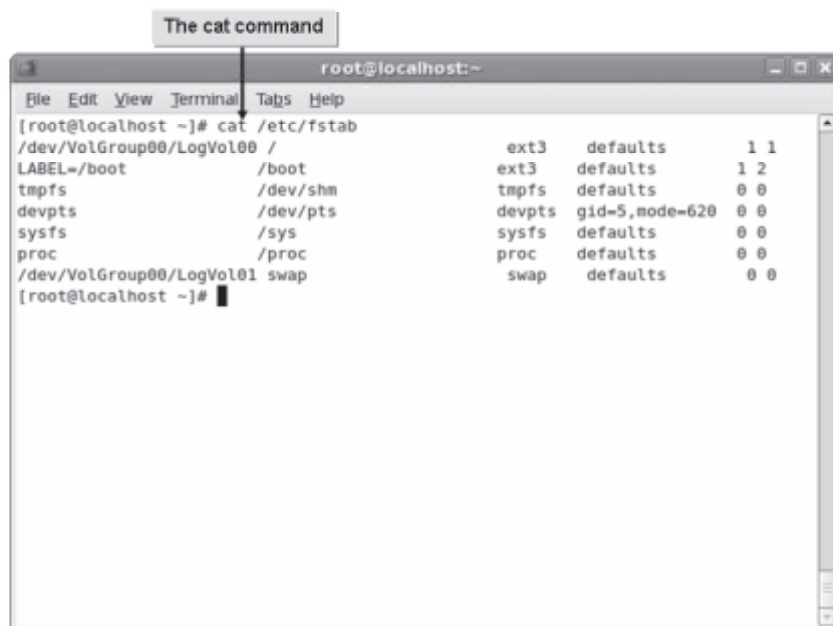


Figure 1-20: *The cat command displaying a text file.*

The `cat` command options are described in the following table.

Option	Description
<code>-n</code>	Precedes the output with its respective line number.
<code>-b</code>	Numbers the lines, excluding the blank lines.
<code>-u</code>	Omits to buffer the output.
<code>-s</code>	Omits to display results for nonexistent files.
<code>-v</code>	Displays nonprinting characters as visible characters, other than tabs, new lines, and form-feeds.
<code>-e</code>	Prints a <code>\$</code> character at the end of each line, prior to the new line.
<code>-t</code>	Prints tabs as <code>^I</code> and form-feeds as <code>^L</code> .

Syntax

The syntax of the `cat` command is `cat [command options] {file name}`.

The which Command

The `which` command is used to verify whether a user has the right to execute a command. It displays the complete path of the command by searching the directories assigned to the `PATH` variable. For example, on entering `which cat`, the following output is displayed:
`/bin/cat`.



Figure 1-21: The `which` command displays the complete path of the command.

How to Enter Shell Commands

Procedure Reference: Log in to Your System

To log in to your system:

1. Log in to the GUI of the system.
 - a. In the **Username** text box, enter the user name.
 - b. In the **Password** text box, enter the password of the user.
2. Log in to the CLI of the Linux system.
 - a. Press **Ctrl+Alt+F1** to switch to the first terminal.
 - b. To log in to the system, enter the user name.
 - c. Enter the password.

Procedure Reference: Monitor User Logins

To monitor user logins:

1. Log in as root.
2. Monitor user logins in the system.
 - To display the login information about the connected users and the processes associated with those users, enter `w`.
 - To display the users who are currently logged in to the system, enter `who`.

Procedure Reference: Check the System Date and Calendar Using Commands

To check the system date and calendar:

1. Log in to the CLI of the Linux system.
2. To view the date details, in the terminal, enter the `date` commands.
 - To check the current date and time on the system, enter `date`.
 - To view the date in the month-date-year format, enter `date +%m-%d-%y`.
 - To view the current time in the hour-minute-second [AM or PM] format, enter `date +%r`.
3. To view a specific calendar, enter the `cal` command.
 - To display the current month's calendar, enter `cal`.
 - To view a specific month's calendar, enter `cal {month} {year}`.
 - To display the calendar in a specific format, enter `cal [option]`.



In addition, in the GUI, you can choose **System**→**Administration**→**Date & Time** to view the system date and time in the **Date/Time Properties** dialog box.

4. If necessary, to clear the terminal screen, enter the `clear` command.

Procedure Reference: Display System Information Using Commands

To display the system information:

1. Enter a suitable command to view specific system information.
 - To check the duration since the system is running, enter `uptime`.
 - To display the history of logins, enter `last`.
 - To display the history of bad logins on the system, enter `lastb`.
 - To display the hostname of the system you are currently logged in to, enter `hostname`.
 - To display the user name with which you are currently logged in, enter `whoami`.

ACTIVITY 1-2


Using Basic Commands

Before You Begin:

- 1. The Red Hat Enterprise Linux 5.3 server is set up and configured to use the GNOME GUI.
- 2. The system is booted and the GUI login screen is displayed.

Scenario:

You have been provided with a Linux system at your workstation and are required to work as a team along with your colleagues who will also access your system from their systems. After logging in to your system, you decide to check the details of the users who are connected to your system to update yourself with the usage of your system.

 Whenever the instruction states “enter *command*”, you are required to type the command and press **Enter**.

What You Do	How You Do It
1. Log in to the GUI as jsmith.	<ul style="list-style-type: none">a. To log in to the system, in the Username text box, type <i>jsmith</i> and press Enter.b. In the Password text box, type <i>myp\$\$w0rd</i> and press Enter.
2. Log in to the first terminal as jsmith.	<ul style="list-style-type: none">a. To switch to the first terminal, press Ctrl+Alt+F1.b. To log in to the first terminal, type <i>jsmith</i> and press Enter.c. Type <i>myp\$\$w0rd</i> and press Enter.d. To view the current date and time of the system, at the command line, enter datee. Observe that the current date and time of the system is displayed.

- | | |
|---|---|
| 3. Log in to the fifth terminal as eric. | <ul style="list-style-type: none"> a. To switch to the fifth terminal, press Ctrl+Alt+F5. b. To log in to the fifth terminal, type <i>eric</i> and press Enter. c. Type <i>myp\$\$\$\$word</i> and press Enter. d. To view the current date and time of the system, enter date e. Observe that the current date and time of the system is displayed. |
| <hr/> | |
| 4. Log in to the sixth terminal as robert. | <ul style="list-style-type: none"> a. To switch to the sixth terminal, press Ctrl+Alt+F6. b. To log in to the sixth terminal, type <i>robert</i> and press Enter. c. Type <i>myp\$\$\$\$word</i> and press Enter. d. To view the calendar for the current month, enter cal e. Observe that the calendar of the current month is displayed. |
| <hr/> | |
| 5. View the list of users who are currently logged in to the Linux system. | <ul style="list-style-type: none"> a. To switch to the first terminal, press Ctrl+Alt+F1. b. To view the list of users who are currently logged in to the Linux system, enter who c. Observe the list of user names displayed in the first column of the command output. |
| <hr/> | |
| 6. Display information about users currently logged in to the Linux system. | <ul style="list-style-type: none"> a. To display information about users currently logged in to the Linux system, enter w b. Examine the USER and WHAT columns to check the names of users logged in currently and obtain information about what each user is doing. c. To clear the terminal screen, enter clear |
-
-

ACTIVITY 1-3

Using System Commands

Before You Begin:

You have logged in as jsmith in the first terminal of the CLI.

Scenario:

After viewing the details of the users connected to your system, you decide to check the details of the system, the duration for which the system is running, and the system date and time.

What You Do	How You Do It
1. Check the name of your Linux system.	<ol style="list-style-type: none">To check the name of your Linux system, at the command line, enter hostnameObserve the hostname of your system.To clear the terminal screen, enter clear
2. Check how long the system has been running and the current date and time.	<ol style="list-style-type: none">To check how long the system has been running, enter uptimeObserve that the first column of the command output displays how long the system has been running.To check the current date and time of your system, enter dateObserve the displayed date and time.
3. Check the current calendar.	<ol style="list-style-type: none">To view the calendar for the current month, enter calObserve the calendar for the current month. Enter cal <year> to view the calendar for the current year.Observe the calendar for the year. To clear the terminal screen, enter clear

TOPIC C

Get Help Using Linux

Now that you are familiar with the Linux shell, you may want to begin using commands in your system. However, you may need assistance with the various commands available. In this topic, you will identify the help and support options offered by Linux.

By learning about Linux support options, you can increase your access to information about the Linux environment. Doing so will help you support your implementation of Linux. The information provided in the Linux documentation will enable you to easily troubleshoot problems you encounter.

Linux Documentation

Definition:

Linux documentation is the material that provides information on various Linux commands and blocks of code. Some Linux documentation is available in electronic format and some in print format. Linux documentation is available from sources such as manual pages, online resources, published works, Usenet newsgroups, and mailing lists.

Example:



Figure 1-22: Built-in Linux help in the GUI.

System Documentation

System documentation is the term given to the collection of documents that list the system requirements; its functioning capabilities, limitations, design specifications; the internal workings of the system; and the steps for maintaining the system.

Manual Pages

The Linux *manual pages*, or man pages, contain the complete documentation that is specific to every Linux command; they are presented in simple ASCII text format. The man page for a specific command is displayed using the `man` command. The man pages are available on the system by default. They usually include information such as the name of the command, its syntax, a description of its purpose, the options it supports, examples of common usage of the command, and a list of related commands.

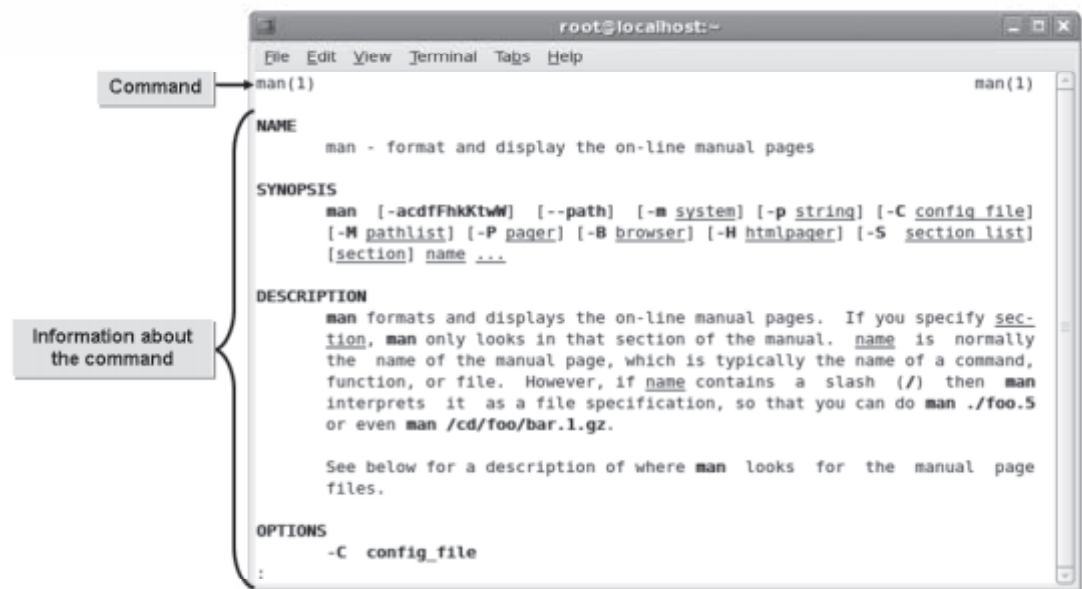


Figure 1-23: Viewing information on the manual pages.

Syntax

The syntax of the `man` command is `man {topic}`.

The man Command Options

The `man` command supports different options. Some of the frequently used options are listed here.

Option	Description
-a	Finds all entries matching the query.
-D	Displays debugging information.
-f	Displays a short description of the command along with the man pages/sections.
-h	Displays help options for the man command.
-k	Lists all manual pages/sections containing the keyword along with their location.
-K	Searches for the specified string on all pages.
-t	Formats the man pages to enable printing.

Man Page Sections

Man pages for a single command may be listed under several sections. All the available manual page sections for a particular command can be listed using the `whatis` command. When a command has more than one section listed, it means that documentation for the same command is available from more than one source. These sections are identified by the number displayed beside the command, for example, `fsck (8)`.

Various man page sections are given in the table below.

Section Number	What It Contains
1	General commands
2	System calls
3	C library functions
4	Special files (usually found in <code>/dev</code>)
5	File formats and conventions
6	Games and screensavers
7	Miscellaneous
8	System administration commands and daemons

Keys to Navigate Through Linux Man Pages

You can navigate through the Linux man pages using a number of keys. The functions of different keys are given in the following table.

Key	Used To
Home	Move to the beginning of the man page.
End	Move to the end of the man page.
Page Up	Scroll up the page progressively.
Page Down	Scroll down the page progressively.
N	Move to the next occurrence of the search term.
P	Move to the previous occurrence of the search term.
Q	Quit and return to the shell prompt.

The apropos Command

The `apropos` command is generally used when a user does not know which command to use to perform a certain action. It can be used with a keyword to display a list of the manual pages containing the keyword along with their man page sections. The `apropos` command searches a regularly updated database called the `whatis` database for the specified string and returns all matching entries.

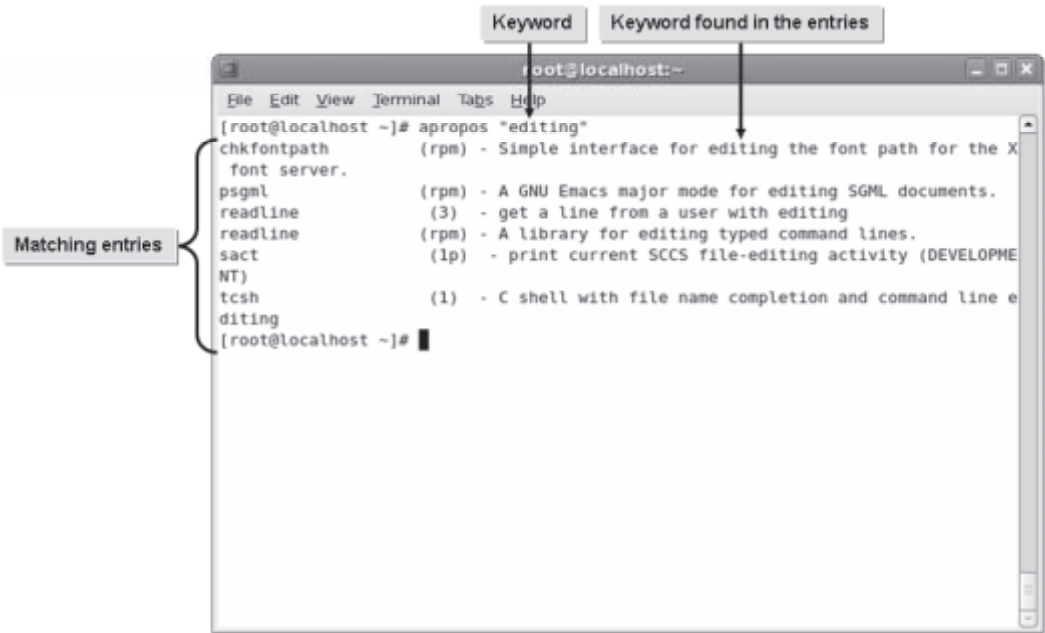


Figure 1-24: Searching for help using the apropos command.

Syntax

The syntax of the apropos command is `apropos {keyword}`.

Other Built-In Help Options

In addition to the man and apropos commands, Linux offers other built-in options for help.

Help Option	Description
whatis	Displays a short description of the command along with the man pages/sections matching the exact command. This command searches a regularly updated database for documentation. The syntax of this command is <code>whatis {command}</code> .
info	Displays info pages containing additional or recent information about a command. The syntax of this command is <code>info {command}</code> .
command --help	Displays a quick summary of the usage of a command and a list of arguments that can be used. This feature can be used with most commands in Linux. The syntax of this command is <code>command -options</code> .

The /usr/share/doc Directory

The /usr/share/doc directory contains documents installed on the system, describing in detail certain aspects of configuring or using Linux.

HOWTOs

HOWTO documents may be installed on your system, usually under the `/usr/share/doc` directory. The HTML version of the files can be displayed in any web browser, including the text-based Lynx browser. The text files can be viewed through any text editor or by using the display commands such as `cat`, `more`, or `less`. HOWTOs can be found on most systems and can also be found on the web at <http://linuxdocs.org/HOWTOs/HOWTO-INDEX/howtos.html> and other sites.

HOWTOs are comprehensive documents, much like FAQs, but generally not in question-and-answer format. However, many HOWTOs contain a FAQ section at the end. There are several HOWTO formats available: plain text, PostScript, PDF, and HTML. In addition to the HOWTOs, there are a multitude of mini-HOWTOs on short, specific subjects.

Getting Help from Info Pages

To display info pages, enter `info`, with or without options and arguments. By itself, the command `info` will display the help file on how to work with info pages. Entering `info [topic]` will display the info page for the specified topic. The command `info --help` displays a brief help description.

When the info page is displayed, any text with an asterisk (`*`) in front of it is a link. Move your cursor (using the arrow keys) to the text, and then press **Enter** to access the linked info page. To return to the previous document, type **U** and then type **D** to return to the top of the page. Type **Q** to return to the command prompt.

LUGs

A good source of information for Linux users and developers is Linux User Groups, or LUGs. These can be virtual (based on the web) or there may be a group of people who meet in your neighborhood. The virtual ones sometimes take the form of a message board with a question-and-answer database.

Online Help

The Internet is the best place to get documentation for any distribution of Linux. There are dedicated websites and online forums that help Linux users with specific distributions or Linux in general. Documentation for commercial distributions is available in their respective official websites. These include the release notes of different versions and updates, the deployment guide, the installation guide, and the virtualization guide. For example, the Red Hat documentation can be accessed from the URL, www.redhat.com/docs/manuals/enterprise.

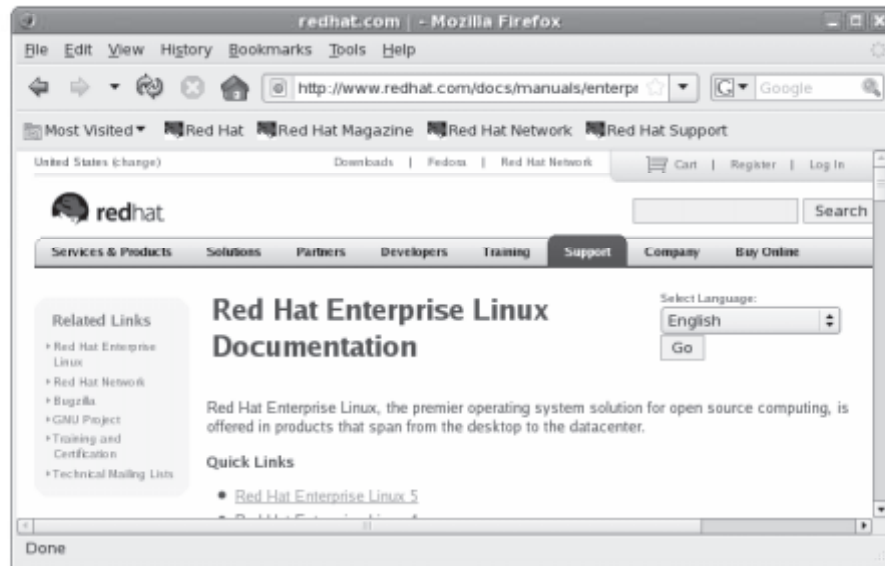


Figure 1-25: The Red Hat online documentation.

How to Access Help in Linux

Procedure Reference: View Linux man Pages

To view Linux man pages:

1. Enter `man {command}` at the command line, where `{command}` is the command for which you want to view the man page.
2. View the list of command options available for the command.
3. Close the man page for the specified command.

Procedure Reference: Display the man Page for a Command

To display the man page for a command:

1. Log in as a user.
2. To display the man page for a specific command under a specific section, enter `man [section] {command}`.
3. Navigate through the man pages.
 - To navigate within a page, use the **Up Arrow** or **Down Arrow** key.
 - To navigate through several pages, use **Page Up** or **Page Down**.
 - Search for some specific topic in the man pages as required.
 - a. To search through the man page for the specified string, enter **/search string**.
 - b. If necessary, to locate the next occurrence of the string in the man page, type **n**.
4. To close the man page, press **Q**.

Procedure Reference: Use the `whatis` Command

To use the `whatis` command:

1. Log in as a user.
2. To build the `whatis` help database, enter `makewhatis`.
3. To display the man page sections and a short description of the specified command, enter `whatis {command name}`.
4. To view the man page for the specified command under the specified section, enter `man [section] {command}`.
5. To close the man page, press **Q**.

Procedure Reference: Find the Relevant man Pages Using the `apropos` Command

To find the relevant man pages using the `apropos` command:

1. Log in as a user.
2. To search the keyword in the `whatis` database and display the matching man page sections for the specified keyword, enter `apropos {keyword}`.
3. To display the man page for a specific command under a specific section, enter `man [section] {command}`.
4. To close the man page and return to the command prompt, press **Q**.

Procedure Reference: Display the Info Documents of a Command

To display the info documents of a command:

1. Log in as a user.
2. To read the info documents for the specified command, enter `info command`.
3. Navigate through the info pages.
 - To navigate within a page, use the **Up Arrow** or **Down Arrow** key.
 - To navigate through several pages, use **Page Up** or **Page Down**.
 - To move to the next or previous page, type `n` or `p`, respectively.
 - To search for a particular string on the info pages, type `s`.
 - To go to the next link, press **Tab**.
4. To close the info page, press **Q**.

Procedure Reference: Display the Options of a Command

To display the options of a command:

1. Log in as a user.
2. To display the command syntax and a list of options, enter `command --help`.
3. To use the necessary option to execute the required task, enter `command -options`.

ACTIVITY 1-4

Identifying Linux Documentation Types and Uses

Before You Begin:

- 1. Press **Ctrl+Alt+F5**.
- 2. Type `logout` and press **Enter** to log out eric from the fifth terminal.
- 3. Press **Ctrl+Alt+F6**.
- 4. Type `logout` and press **Enter** to log out robert from the sixth terminal.
- 5. Press **Ctrl+Alt+F1**.

Scenario:

Your manager, Linda, is having trouble understanding certain commands. She knows that there are several types of support documentation available, but is unsure of how to use them. She also heard that a large part of the hidden cost involved with implementing Linux is a result of limited support. She would like you to submit a report on the different types of Linux documentation and their uses. You decide to explore the available help options.

What You Do	How You Do It
1. Display the manual for the <code>gzip</code> command.	<ul style="list-style-type: none">a. At the command line, enter <code>man gzip</code>b. To continue reading through the man page, press the Spacebar.c. To return to the command line, press Q.
2. Build the <code>whatis</code> database.	<ul style="list-style-type: none">a. To log out <code>jsmith</code>, enter <code>logout</code>b. To log in as <code>root</code>, enter <code>root</code>c. At the Password prompt, enter <code>p@ssw0rd</code>d. To build the <code>whatis</code> database, enter <code>makewhatis</code>
3. Search through the man pages for the word "zip."	<ul style="list-style-type: none">a. Enter <code>apropos zip</code>b. Observe that the output lists all the instances where the keyword "zip" is found.

4. View the list of locations where the keyword is found in the man pages.
 - a. At the command line, enter **whatis gzip**
 - b. View the results.
 - c. To clear the terminal screen, enter **clear**

 5. True or False? It is common practice to write a detailed report of exactly what is installed and changed on each Linux system in your environment.
☐ True
☐ False

 6. What are the additional help options that may be installed on your Linux system?
 - a) --help
 - b) helpme
 - c) HOWTO
 - d) Textinfo

 7. In what formats are HOWTOs available?
 - a) PostScript
 - b) Email
 - c) PDF
 - d) HTML
-
-

ACTIVITY 1-5

Getting Help Using Linux Manual Pages

Before You Begin:

You have logged in as root in the CLI terminal

Scenario:

Your organization supports customers around the world and you may have to support different customers with varying time zones. To achieve this, your system time should correspond to the time on your clients' systems. You are unsure about the procedure to change the system date and time. You decide to browse the manual pages to find more help.

LESSON 1

What You Do	How You Do It
1. Find the man page for the <code>date</code> command.	<ul style="list-style-type: none">a. To see the relevant man pages for the <code>date</code> command with various sections, enter <code>whatis date</code>b. To see the man page of the <code>date</code> command under section 1, enter <code>man 1 date</code>
2. Search through the man page.	<ul style="list-style-type: none">a. To move to the first instance of the text "FORMAT," enter <code>/FORMAT</code>b. To navigate to the next instance of the text "FORMAT," enter <code>/</code>c. To view the different formats allowed for the <code>date</code> command, enter <code>/</code>d. To close the <code>date</code> man page, press <code>Q</code>.
3. View the info page.	<ul style="list-style-type: none">a. To view the complete info document for the <code>date</code> command, enter <code>info date</code>b. To navigate to the text "Examples," press <code>/</code> and enter <code>Examples</code>c. To navigate to the next instance of the text "Examples," press <code>/</code> and press <code>Enter</code>.d. To view examples of the <code>date</code> command, press <code>Enter</code>.e. Observe the first three examples of the <code>date</code> command.f. To close the info page, press <code>Q</code>.g. To clear the terminal screen, enter <code>clear</code>

TOPIC D

Start and Stop Linux

In the last topic, you identified the help and support options offered by Linux and accessed documentation in the shell. But you cannot troubleshoot system problems without knowing how to start and stop your system. In this topic, you will start and stop the Linux system.


We all expect our operating systems to load and run the necessary processes at boot time. There are occasions, however, when you, as a Linux administrator, may want to start, stop, or restart the system manually. The ability to manage these essential services will help you perform maintenance and upgrades on your system.

Services

Definition:

A Linux *service* is an application or set of applications that perform tasks in the background. The services running on a Linux system range from basic services to server services. Services can be broadly classified as critical services and noncritical services. Critical services are the core services that are vital for the functioning of the Linux system. Noncritical services are services that are initiated by applications installed on the system.

Example:



```
root@localhost:~  
File Edit View Terminal Tabs Help  
[root@localhost ~]# service network status  
Configured devices:  
lo eth0  
Currently active devices:  
lo eth0  
[root@localhost ~]#
```

Figure 1-26: The network service displaying its status.

The service Command

The `service` command allows you to manage services running on your system. The syntax of `service` command is: `service {service name} {options}`.

Daemons

Definition:

A *daemon* is a program that runs in the background without the need for human intervention, often handling commands delivered for remote command execution. It lies dormant until an event triggers it into activity. Some daemons operate at regular intervals. Most daemons are started when the system boots. Daemons are started either by the operating system, by applications, or manually.

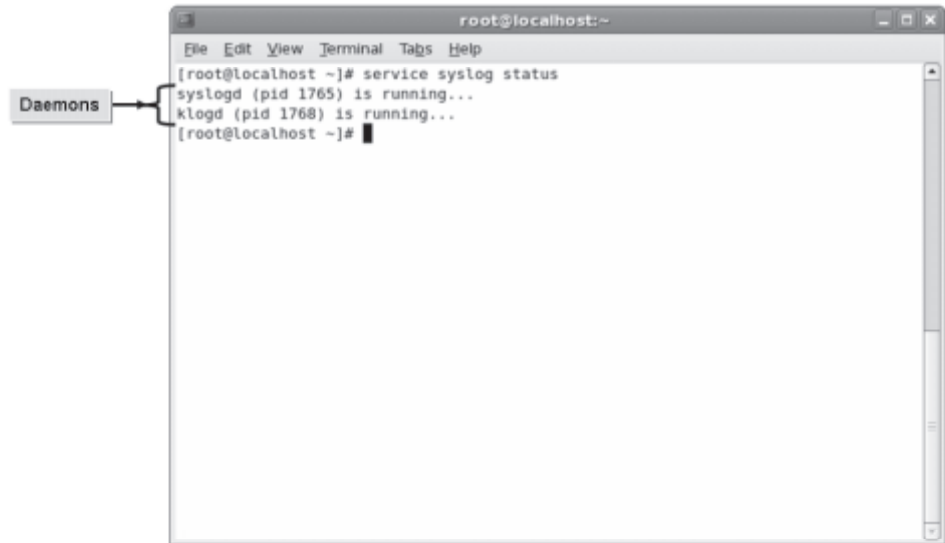


Figure 1-27: Daemons running in the background for the syslog service.

Example: lpd

The Line Printer Daemon, or `lpd`, controls the flow of print jobs to a printer. It works in the background and sends the output to the printer without affecting other processes that a user is working on at that time.

Init Runlevels

Init is used to set the *runlevel* of your system. The runlevel specifies the group of processes that can exist. *Init* creates processes at system boot time from a script in the `/etc/inittab` file. You can change the current runlevel by using the `telinit` command. The `init` man page says “Init is the parent of all processes.”



Figure 1-28: The different runlevels that can be specified with the *telinit* command.

Init Runlevels Table

The following table describes the processes that can run at each init level.

Init Level	Description
0	Halts the system
1	Single-user mode
2	Multiuser mode without networking
3	Multiuser mode with networking
4	User configurable
5	Used for the GUI (X11 multiuser mode)
6	Reboots the system

The Upstart Init Daemon

The traditional System V (SysV) UNIX init system has been replaced by an improved version of init known as *Upstart*. The Upstart init system is event-based rather than runlevel-based. Event-based means that jobs will be automatically started and stopped by changes to the system's state. The original SysV init was dependency-based and jobs had to start in a particular order. The Upstart init daemon doesn't track runlevels. Runlevels are tracked by the runlevel event generated by telinit or shutdown. The init daemon sets two environment variables from the runlevel event: `RUNLEVEL` and `PREVLEVEL`. These environment variables are the current runlevel and the previous runlevel. Upstart's list of configuration files is located in the `/etc/init` directory.

The Systemd Init Daemon

Systemd is a replacement for Upstart in some Linux distributions. It allows for greater concurrency (starting programs at the same time for quicker boot) and reduces shell overhead. Systemd has some advantages over the SysV init and Upstart init systems by allowing socket-activated and bus-activated services. Control Groups (cgroups) are used to track processes instead of Process IDs (PIDs), which provides better isolation for processes.

System Booting

During the installation of Linux, the boot loader you choose will be put on the *Master Boot Record (MBR)*. GRand Unified Bootloader (GRUB) is the Linux boot loader that loads and starts the kernel. Only one boot loader can be used on a system.

Boot Loader

A boot loader is a program that loads the kernel so that Linux and other operating systems can boot.

System Shutdown

The *shutdown* command is used to close a system. This closes files and performs other tasks necessary to safely shutdown the system. It warns all users that the system is going to shutdown and no one can log in after the command is issued. After certain installations or removal of hardware, it is necessary to shutdown the Linux system.

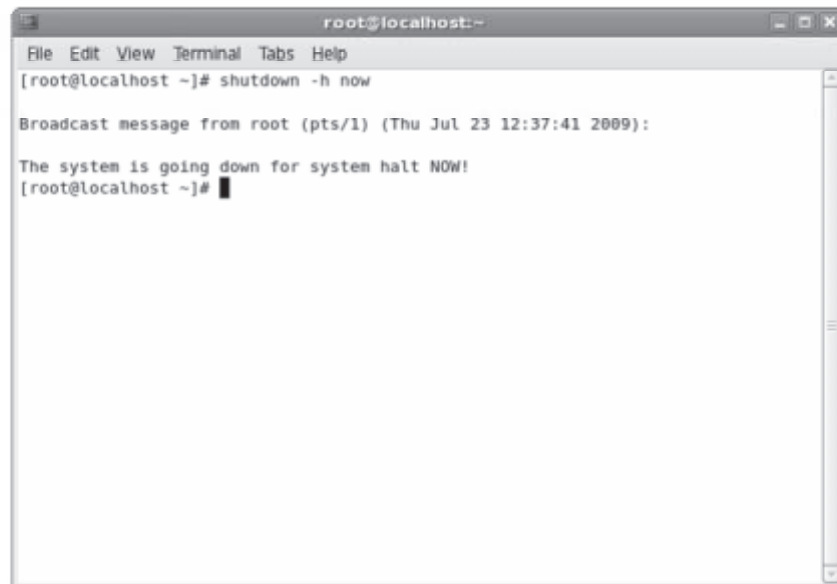


Figure 1-29: Shutting down a Linux system.

Shutdown Command Options

When you need to restart your Linux system, you should use the *shutdown* command with the appropriate options. The syntax of the *shutdown* command is `shutdown [-t seconds] [-options] time [warning message]`.

The *-t* option specifies how many seconds to wait before changing to another runlevel. The other options are listed in the following table.

Option	Used To
-k	Send warning messages to everyone, but does not really shut-down the system.
-r	Reboot the system after shutdown. Upon reboot, if you are using a boot manager to load various operating systems, you can switch to another operating system or log in to Linux.
-h	Halt the system after shutdown. At this point, you can safely turn off the power.
-n	Shutdown the system without invoking init. It is recommended not to use this option.
-f	Skip the filesystem check on reboot.
-F	Force the filesystem check on reboot.
-c	Cancel a shutdown in progress. This option does not use the time parameter, but can use the warning message option.

How to Start and Stop Linux

Procedure Reference: Manage Runlevels from a Shell

To manage runlevels from a shell:

1. At the command prompt, bring up your current runlevel.
2. Switch to runlevel 1.
3. Verify that you are at runlevel 1.
4. Exit back to runlevel 3.

Procedure Reference: Manage Runlevels from a Configuration File

To manage runlevels from a configuration file:

1. Edit the `/etc/inittab` file to start at runlevel 1.
2. Restart the computer.
3. Verify that you are in runlevel 1.
4. Edit the `/etc/inittab` file to start at runlevel 3.
5. Restart the computer.

Procedure Reference: Alert Users Before Switching Runlevel

To alert all users connected to your system before switching runlevel:

1. Log in as root in the CLI.
2. Enter `shutdown -t [seconds] now [message]` or enter `shutdown -k now`.

The `/etc/nologin` File

When the shutdown program is called with a delay, it will create an empty `/etc/nologin` file, which will restrict further connections. If you manually add this file, it will allow only the superuser or root user to log in and restrict all others. The contents in the `/etc/nologin` file will be displayed on every failed login attempt.

ACTIVITY 1-6

Starting and Stopping Linux

Before You Begin:

You have logged in as root in the CLI.

Scenario:

You are given the task of managing the implementation of Linux at your company. To begin, you must learn to start and stop your Linux system and familiarize yourself with various runlevels.

What You Do	How You Do It
1. Examine various runlevels.	<ol style="list-style-type: none">At the command line, enter more /etc/inittabPress the Spacebar two times to continue.Observe the contents of the <code>/etc/inittab</code> file displayed on the monitor.To determine your current runlevel, enter runlevelObserve your current runlevel.

2. Switch to the single-user mode.
 - a. At the command line, enter **telinit 1**
 - b. Observe that the services of the previous runlevel are stopped and runlevel 1 service has started.
 - c. To verify that you are in single-user mode, enter **runlevel**
 - d. Observe that the command shows 1 S, for single user 1. To return to the default runlevel, which is runlevel 5, enter **exit**
 - e. To switch to the first terminal of the CLI, press **Ctrl+Alt+F1**.
 - f. At the **login** prompt, enter **root**
 - g. At the **Password** prompt, enter **p@ssw0rd**

 3. Restart the Linux system.
 - a. At the command line, enter **shutdown -r now**
 - b. Observe that the system sends a broadcast message from root, the current user, to the other users connected to the system to indicate that it will be rebooted.
 - c. Observe that the services are stopped and processes are killed before restarting the system. To switch to the first terminal of the CLI, press **Ctrl+Alt+F1**.
 - d. Log in to the system as **root** with the password as **p@ssw0rd**
-

Lesson 1 Follow-up

In this lesson, you identified basic Linux concepts and performed basic Linux tasks. These skills can assist you in supporting Linux users and machines.

1. What are the advantages of open source software over licensed software?

LESSON 1

2. What are the advantages of using Linux?

LESSON 2

Managing User and Group Accounts

Lesson Time

1 hour(s), 15 minutes

In this lesson, you will manage user and group accounts.

You will:

- Create user and group accounts.
- Configure user profiles.
- Manage user and group accounts.

Introduction

You are now familiar with the history of Linux, its shells, and its help and support options. This basic knowledge is a good starting point, but there is more to learn. Before users can take advantage of the operating system, user accounts need to be created. You will also have to create group accounts to manage those users. In this lesson, you will manage user and group accounts.

This lesson covers all or part of the following CompTIA Linux+ Powered by LPI certification objectives:

- Topic A:
 - Objective 107.1, Objective 110.1, Objective 110.2
- Topic B:
 - Objective 103.1, Objective 105.1, Objective 107.1
- Topic C:
 - Objective 107.1, Objective 110.1

One of the benefits of Linux is its multiuser capabilities. By creating and modifying user and group accounts, you can further tailor the Linux environment to the needs of your organization. You will also be able to provide individualized services to users after creating an account for them.

TOPIC A

Create User and Group Accounts

In this lesson, you will manage user and group accounts. The first step in managing them is to create the accounts you need. In this topic, you will create user and group accounts.

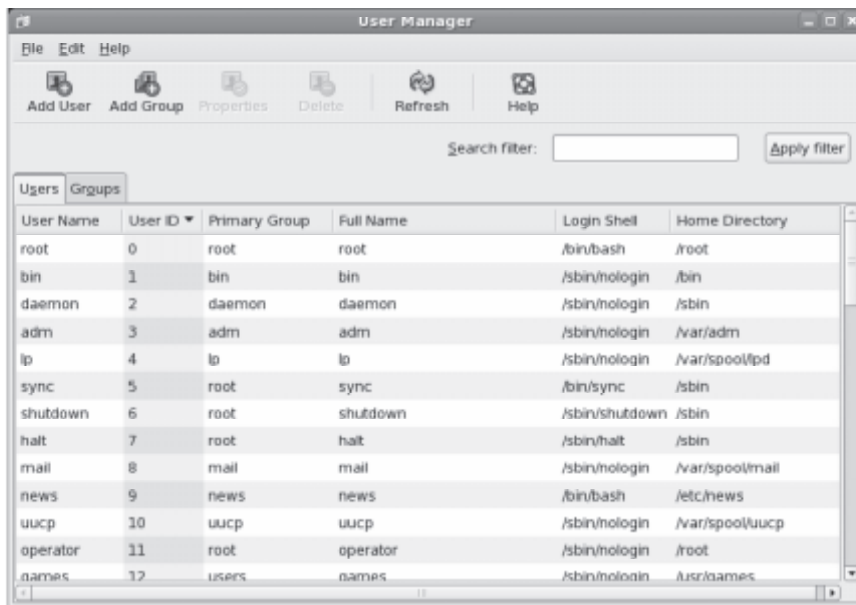
As a Linux administrator, you will be required to create user and group accounts on a regular basis. By creating user accounts, you will enable users to access the Linux system. Group accounts enable you to group users with similar functions. This will considerably reduce the time and effort you invest in monitoring and managing user activities.

User Accounts

Definition:

A user account is a collection of information that defines a user on a system. It is the representation of a user on a computer. User account information includes the user name and password for the user to log in to the system, groups to which the user belongs, and rights and permissions that the user has to access the system and its resources. When an account is created, it is assigned a unique number that is called User ID (UID).

Example:



The screenshot shows a window titled "User Manager" with a menu bar (File, Edit, Help) and a toolbar with icons for Add User, Add Group, Properties, Delete, Refresh, and Help. Below the toolbar is a search filter input field and an "Apply filter" button. The main area has two tabs: "Users" (selected) and "Groups". The "Users" tab displays a table with the following data:

User Name	User ID	Primary Group	Full Name	Login Shell	Home Directory
root	0	root	root	/bin/bash	/root
bin	1	bin	bin	/sbin/nologin	/bin
daemon	2	daemon	daemon	/sbin/nologin	/sbin
adm	3	adm	adm	/sbin/nologin	/var/adm
lp	4	lp	lp	/sbin/nologin	/var/spool/lpd
sync	5	root	sync	/bin/sync	/sbin
shutdown	6	root	shutdown	/sbin/shutdown	/sbin
halt	7	root	halt	/sbin/halt	/sbin
mail	8	mail	mail	/sbin/nologin	/var/spool/mail
news	9	news	news	/bin/bash	/etc/news
uucp	10	uucp	uucp	/sbin/nologin	/var/spool/uucp
operator	11	root	operator	/sbin/nologin	/root
games	12	users	games	/sbin/nologin	/usr/games

Figure 2-1: The format in which the user account information is stored by a system.

The useradd Command

The `useradd` command is used to add a new user. You need to specify the user name along with the command to create a new user account. Special user accounts are required to run processes associated with certain services. For example, `daemon` is a user account that is used to run the daemon service.



```
root@localhost ~]# useradd pat
```

Figure 2-2: A new user added using the `useradd` command.

 You can use the `adduser` command to perform the same functions as the `useradd` command.

Syntax

The syntax of the `useradd` command is `useradd [options] {username}`.

Special User Accounts

In special user accounts, the UID value for the users will be less than the default UID value, which is 500. Such special users will not have a home directory. You can create a special user account using the `useradd -r {special user name}` command.

User Accounts

Linux allows you to add user accounts by directly editing the password file. However, this is not recommended because you may damage your system if you accidentally leave something out or alter existing user accounts. If the system is damaged, nobody will be able to log in—not even the root user. In such a case, you will have to reinstall your system and redefine the user accounts.

Default User Accounts

Numerous user accounts are created by default upon system installation. Some of the main user accounts are:

- root
- bin
- daemon
- ftp
- sshd
- nfsnobody
- apache
- And, squid

The Role of the Root

Every Linux system has at least one system administrator whose job is to maintain the system and make it available to users. This user is the root. The root user can perform any task on the Linux system without restrictions. System administrators are also responsible for adding new users to the system and for setting up their initial environment.

Other Types of User Accounts

The other types of user accounts are:

- Local—Local user accounts allow users to log in to single, specific computer systems.
- Domain—Domain user accounts allow users to log in to a computer system. However, the identity of a user is recognized by all computers in the domain.
- Guest—Guest accounts are built-in user accounts created at the time of installation. They are also known as anonymous accounts. Using an anonymous account, multiple users can log in to the system at the same time. Usually, anonymous accounts do not require passwords.


Passwords

A password is an entity that allows the Linux system to authenticate a user. Generally, when user accounts are created without passwords, they can be easily misused. For this reason, when you create a user account, you should immediately set a password for the user using the `passwd` command. In Linux, if a password is not set for the user account, the account gets locked automatically. This is to help prevent unauthorized access to the system.



```
[root@localhost ~]# passwd pat
Changing password for user pat.
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
[root@localhost ~]#
```

Figure 2-3: Setting a password for the user *pat*.

 You can change the password of your user account using the `passwd` command. You cannot change the password for any other user account because the `passwd` command does not allow you to specify any other user name. Only the root user can change the password for other users by specifying the user name with the `passwd` command.

Syntax

A root user can create a password for a user by entering `passwd [user name]`, where `[user name]` is the name of the user for whom the password is set.

Dictionary Words as Passwords

If you enter a password that is a real word made up solely of alphabetic characters, you will get a bad password message stating that it is based on a dictionary word. The password will still be assigned even though the message is displayed. It is strongly advised that you change it to a more secure password.

The `/etc/passwd` File

When you add a new user, information about the user is saved in the `/etc/passwd` file.

There are various fields in the `/etc/passwd` file.

Field	Description
User name	Stores the user name with which the user logs in to the system. It is recommended to limit user names to eight alphanumeric characters.
Password	Stores the password that is assigned to the user in an encrypted form.
User ID	Stores the unique number that is assigned to each user. Linux tracks users by the UID rather than the user name.
Group ID	Stores the unique number that is assigned to each group. Users can be members of one or more groups.
Full name	Stores the real name of the user.
Home directory	Displays the default directory where the user is placed after logging in.
Login shell	Displays the default shell that is started when the user logs in.

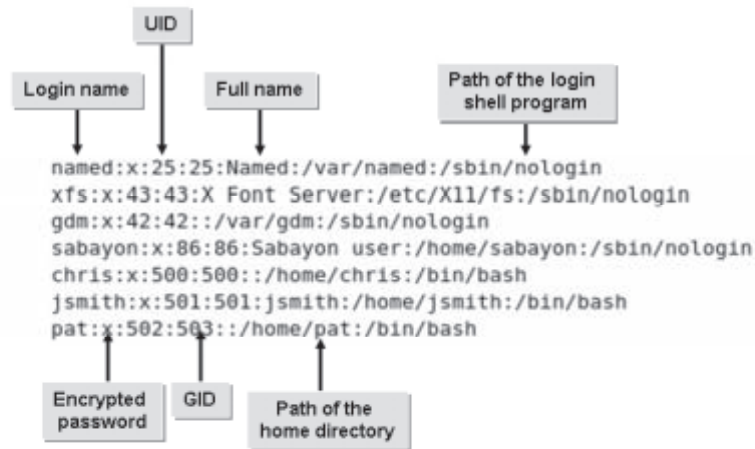


Figure 2-4: *The contents of the /etc/passwd file.*

Shadow Passwords

Each user's password is stored and encrypted in the /etc/passwd file. This file needs to be readable, which makes copies of users' encrypted passwords easily obtainable to any person trying to attack the system. Then, by using various techniques, the attackers can decipher passwords. You can overcome this problem by using shadow passwords. Shadow passwords store the encrypted passwords in a separate highly protected file, the /etc/shadow file. This file is readable only to the root user. Therefore, it is less of a security risk compared to the /etc/passwd file because it becomes difficult for attackers to access the file, obtain the user passwords, and then decipher them. The /etc/passwd file also contains the account or password expiration values.

The /etc/shadow File

The /etc/shadow file contains the following information:

- username: The user name.
- passwd: The encoded password.
- last: Number of days since the password was last changed.
- may: Number of days before which the password may be changed.
- must: Number of days after which the password must be changed.
- warn: Number of days pending before which the password will expire.
- expire: Number of days after which the password will expire and the user account will be disabled.
- disable: Number of days since Jan 1, 1970, that the user account has been disabled.
- reserved: A reserved field.

The id Command

The `id` command is used to display UID and group ID (GID) information. Entering the command with no options displays information about the user who is currently logged in. You can also specify a user name as an option to display ID information about a specific user.

The finger Command

The `finger` command is used to display information about users, including login name, real name, terminal name, write status, idle time, login time, office location, and office phone number. Some of these fields may be empty if no information was included when the user account was created. You can also view information about a specific user by entering `finger [user name]`.

Groups

Definition:

A *group* is a collection of system users having the same access rights. Every user must be a member of a group. Users can also be members of more than one group. Group membership is used to limit access to files and system resources. The `groupadd` command allows you to add a group.

Example:

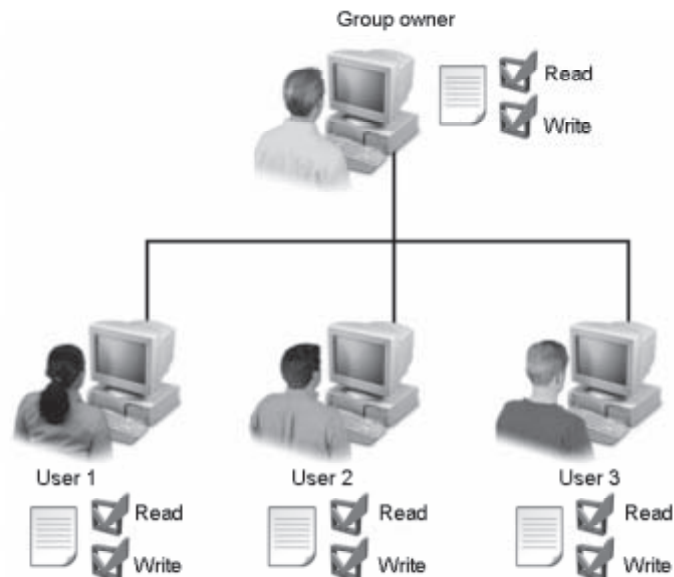


Figure 2-5: A group of users with their permissions.

Syntax

The syntax of the `groupadd` command is `groupadd {group name}`.

Standard Groups

The table lists the standard groups set up by the installation process.

Group	GID	Default Member
root	0	root
bin	1	root, bin, and daemon
daemon	2	root, bin, and daemon
sys	3	root, bin, and adm
adm	4	root, adm, and daemon

Group	GID	Default Member
tty	5	None
disk	6	root
lp	7	daemon and lp
mem	8	None
kmem	9	None
wheel	10	root
mail	12	mail
news	13	news
uucp	14	uucp
man	15	None
games	20	None
gopher	30	None
dip	40	None
ftp	50	None
nobody	99	None
users	100	None

User Private Groups

A *User Private Group (UPG)* is a unique group that is created by default whenever a new user account is created. This is the primary group of the new user account. Only the new user is a member of this group.

The /etc/group File

The */etc/group* file contains a list of groups, each on a separate line. Each line consists of four fields for attribute definition, separated by colons. The */etc/group* file is also termed as the *group database*.

 The */etc/gpasswd* file stores the encrypted passwords for groups.

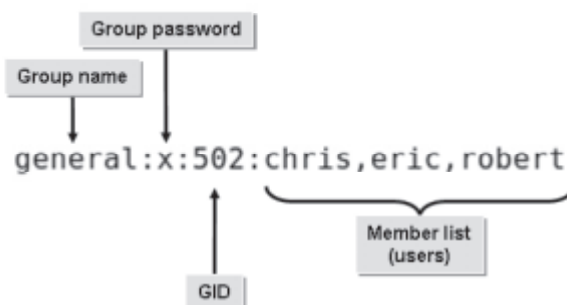


Figure 2-6: An example of an entry in the */etc/group* file.

The following table lists the different fields and their usages.

Field	Description
Group name	Stores the name of the group.
Group password	Stores the password of the group in an encrypted form.
GID	Stores the group identifier; similar to a UID for groups. The default GID value is 500.
Members	Stores the names of the members of the group separated by commas.

How to Create User and Group Accounts

Procedure Reference: Create a User Account

To create a user account:

1. Log in as root in the CLI.
2. To add a new user, at the command prompt, enter `useradd {user name}`.
3. To set a password for the user, enter `passwd {user name}`.
4. Confirm the password.
5. If desired, to log in to the system, use the newly created user name and password.



While creating a user with the `useradd` command, a user private group with the same name is also created.

Procedure Reference: Create a Group Account

To create a group account:

1. Log in as root in the CLI.
2. To add a new group, at the command prompt, enter `groupadd {group name}`.
3. Verify that the group was created by viewing the `/etc/group` file.

ACTIVITY 2-1

Creating User and Group Accounts

Before You Begin:

You have logged in as root in the CLI of srvA.

Scenario:

Two new employees joined your company and their user accounts need to be created. Also, there has been a major reorganization in your company. Your manager would like you to create departmental groups according to the new structure.

User account details:

- User name for the new account: chris
- Password for chris: myp@\$w0rd
- User name for the new account: pat
- Password for pat: myp@\$w0rd
- New groups to be created along with their GID numbers: IT_Support (544), Customer_Support (545), Programming (546), and Design (547)

What You Do	How You Do It
1. Add two new users chris and pat.	<ol style="list-style-type: none">To add a new user, at the command line, enter adduser chrisTo change the password for the user, enter passwd chrisTo assign the new password, enter myp@\$w0rdTo confirm the password, enter myp@\$w0rdObserve that the password is updated successfully.To add another user, enter adduser patTo change the password for the user, enter passwd patTo assign the new password, enter myp@\$w0rd two times.

2. Add user groups IT_Support, Customer_Support, Programming, and Design with the GID numbers specified.
 - a. To add a new group, enter **groupadd -g 544 IT_Support**
 - b. To add the second group, enter **groupadd -g 545 Customer_Support**
 - c. To add the third group, enter **groupadd -g 546 Programming**
 - d. To add the fourth group, enter **groupadd -g 547 Design**

 3. Check that the users' accounts and groups are created.
 - a. To view the group accounts on your system, enter **tail /etc/group**
 - b. Observe that the newly added groups are displayed and have been added to the list of groups.
 - c. Observe that the user accounts have a default group created with the same name as the user.
 - d. To view the user accounts, enter **tail /etc/passwd**
 - e. Observe that the newly added users are displayed and have been added to the list of users.
 - f. To clear the terminal screen, enter **clear**
-
-

TOPIC B

Configure User Profiles

Now that you can create user and group accounts, the next step is to configure user profiles. Each user connected to a system requires a distinct identity to differentiate one user from another. In this topic, you will configure user profiles.

All users connected to the system require customized settings for their systems. Further, there may be files to be shared by default. By configuring user profiles, every user can be given a distinct identity. This differentiates one user from another.

User Profiles

Definition:

A *user profile* is a set of options, preferences, bookmarks, and other user items that characterize a user. User profiles define settings such as network resources, data, attributes, and permissions that the system assigns to a user. These settings are retained for every session. The user can specify a name for the user profile. Otherwise, the profile will be called “Default User.” Each user can create several user profiles for business or personal use.

Example:



Figure 2-7: The list of values set for the root user profile.

Modifying Default Options

You can modify default options while configuring a user profile. Some commonly modified options include:

- **PS1**—This variable stores information about the primary prompt, which is the prompt that is displayed when users log in. This variable may or may not be modified.
- **PS2**—This variable stores information about the secondary prompt.
- **PATH**—This variable stores information about the search paths for commands. You can modify the PATH if you want to use commands that are not stored in the standard directories.

Hidden Files and Directories

Some files and directories in the system are hidden. The `ls` command lists all files, except hidden files. To display all files, including hidden ones, the `ls -a` command is used. The names of hidden files and directories start with a period. You can also add a period to the names of directories to hide them. Hidden files are usually those files that require minimal editing.

The Profile File

When a user logs in and starts a new Bash session, several commands need to be typed to customize the user's session. It will be tedious to type these commands every time the user logs in. Therefore, these commands are saved in a special executable file from where Bash will run the commands every time the user logs in. This file is called a *profile file* because it contains the commands that are used to tailor the session according to the requirements of the user. Individual profiles for every user are available at the `~/.bash_profile` file in the user's home directory, and changes to this file affect the user's customized settings.

Global User Profiles

Definition:

A *global user profile* is a set of options, preferences, bookmarks, stored messages, attributes, permissions, and other user items that users have access to, on whichever system they log in to. Global user profiles are stored on the server. Each time a user logs in, data in the global profile is copied to the local system. While the user is logged in, any changes made to the settings affect only the local copy of the profile.

Example:



Figure 2-8: A global user profile allows the user to access any system connected to the server in which the profile is saved.

Skel Directories

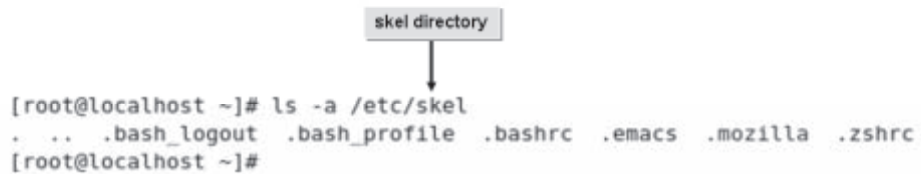
Definition:

When a new user account is created, the *skel directory* stores a copy of the files and directories that are placed in the home directory of the new user. The skel directory path is `/etc/skel`. This ensures that all new users begin with the same settings. Modifications made to the skel directory affect only the new users.



Skel is derived from the word “skeleton,” which implies a basic folder structure.

Example:



```
[root@localhost ~]# ls -a /etc/skel
.  ..  .bash_logout  .bash_profile  .bashrc  .emacs  .mozilla  .zshrc
[root@localhost ~]#
```

Figure 2-9: Default files in the skel directory.

Managing the /etc/skel Files

By default, the hidden files for configuring a user's environment are stored in the skel directory. These include `.bash_profile`, `.bashrc`, `.screenrc`, and others. If there are other files that you would like to include in new user accounts, you can add those files to this directory. The files will then be copied to the new users' home directories when new users are created.

How to Configure User Profiles

Procedure Reference: Maintain skel Directories for New User Accounts

To maintain skel directories for new user accounts:

1. Log in as root in the CLI.
2. Enter `cd /etc/skel`.
3. Enter `gedit .bash_profile`.
4. Make the necessary changes, such as changing `PS1`, `PS2`, or the `PATH` variable for a new user account.
5. Save and close the file.

The Gedit Editor

Gedit is a simple yet powerful GUI-based text editor used in the GNOME desktop. In the GUI environment, you can use the `gedit {file name}` command to open a specific file. Alternatively, you can choose **Applications**→**Accessories**→**Text Editor** to launch the gedit application and use the GUI components to open a specific file.

Procedure Reference: Delegate Files to New Users

To delegate a file to a newly created user by default:

1. Log in as root in the CLI.
2. Enter `cd /etc/skel`.
3. To move the file as a hidden file, enter `mv /[location of the file]/[file name] .[file name]`.
4. Verify that the files have moved as hidden files.
 - a. Create a user.
 - b. Log in as the new user.
 - c. To view the file that was placed in the `/etc/skel` directory, enter `cat .{file name}`.

Procedure Reference: Change a User's Profile

To change a user's profile:

1. Log in as a user.
2. Enter `vi .bash_profile`.
3. Make the necessary changes to a variable and export it. For example, to change the number of commands to be stored in the history variable, specify the desired size in the HISTSIZE variable as `HISTSIZE = {desired value}` and type `export HISTSIZE` to export the variable.
4. Save and close the file.

Procedure Reference: Set the Command Search Path with the Proper Directory

To set the command search path with the proper directory so as to execute the command from anywhere:

1. Log in as a user.
2. Enter `mkdir {directory name}`.
3. Create or add an executable file in the directory.
4. If necessary, to observe the output of the executable file, enter `./{executable file name}`.
5. Enter `vi .bash_profile`.
6. In the PATH variable, type `:$HOME/{directory name}`. For example, if the PATH variable is given as `PATH=$PATH:$HOME/bin`, then after adding the command search path, the PATH variable will look like `PATH=$PATH:$HOME/bin:$HOME/{directory name}`.
7. Save and close the file.
8. Log out and log in as the same user.
9. To execute the file, enter `{executable file name}`.

The which Command

The `which` command is used to verify whether a user has the right to execute a command. The `which` command displays the complete path of the command by searching in the PATH variable. For example, on entering `which cat`, the output `/bin/cat` is displayed.

This means that the `cat` command is located in the `/bin` directory. If `/bin` is not located in the PATH variable, an error message saying “no cat in [search path]” is displayed.

Procedure Reference: Manage env Variables Globally

To manage an env variable globally:

1. Log in as root in the CLI.
2. If desired, to observe the settings, enter `env | less`.
3. Enter `vi /etc/profile`.
4. To define a variable, enter `{VARIABLE NAME}={value}`.

5. If necessary, you can modify the values of the variables. For example, to modify the HISTSIZE profile globally for all users, navigate to the HISTSIZE variable and make the necessary changes.
6. To export the variable, type `export {VARIABLE NAME}`.
7. Save and close the file.
8. Log out and log in as root.
9. If necessary, to observe the changes made to the settings, enter `env | less`.

Procedure Reference: Manage the set Variable

To manage the set variable:

1. Log in as root in the CLI.
2. If necessary, to observe the set variables, enter `set | less`.
3. If necessary, to verify the output, enter `echo $Set variable {VARIABLE NAME}`.
4. Enter `vi .bash_profile`.
5. To define a variable, enter `Set variable {VARIABLE NAME} = {value}`.
6. To export the variable, type `export {VARIABLE NAME}`.
7. Save and close the file.
8. Log out and log in as root.
9. If desired, to verify the changes, enter `set | less`.

The unset Command

The `unset` command is used to remove the set variables temporarily.

ACTIVITY 2-2

Configuring User Profiles

Data Files:

- Desktoppolicies.txt

Before You Begin:

1. You have logged in as root in the CLI of srvA.
2. At the command line, enter
`cp /085099Data/Managing_Users_and_Groups/* /root.`
3. To clear the terminal screen, enter `clear`.
4. Switch to the GUI.
5. Log in as root.

Scenario:

You are assigned the task of creating user accounts and configuring user profiles for employees in a startup company, Our Global Company (OGC) Products. Based on the new company's policy, all new user accounts should be provided with the Desktoppolicies.txt manual, and the user's command prompt should display the company name along with the user name.

The Desktoppolicies.txt file is located in the root directory.

The company name is "OGC Products."

User account details:

- User name for the account to be created: newuser
- Password for the newuser: myp@\$w0rd

What You Do	How You Do It
1. Move the Desktoppolicies.txt file as a hidden file.	<ol style="list-style-type: none"> a. Choose Applications→Accessories→Terminal. b. To switch to the skel directory, in the root@localhost window, enter <code>cd /etc/skel</code> c. To view the hidden files, enter <code>ls -a1</code> d. To move the Desktoppolicies.txt file as a hidden file, enter <code>mv /root/Desktoppolicies.txt .Desktoppolicies.txt</code>

LESSON 2

2. Display the user name along with the company name at the command prompt.
 - a. Enter **gedit .bash_profile**
 - b. To move to a new line at the end of the file, press **Ctrl+End**.
 - c. To change the primary prompt, enter **PS1="[OGC Products/ \u] "**
 - d. Save the file and close the gedit window.
 - e. Clear the terminal screen.

3. Assign the .Desktoppolicies.txt file to the **newuser** account.
 - a. To add the newuser account, enter **useradd newuser**
 - b. To set a password for newuser, enter **passwd newuser**
 - c. To assign the password, enter **myp@\$w0rd**
 - d. To confirm the password, enter **myp@\$w0rd**

4. Check that the file has been moved.
 - a. To switch to the first terminal, press **Ctrl+Alt+F1**.
 - b. Log out **root**.
 - c. Log in as **newuser**.
 - d. Observe that the company name is displayed.
 - e. To verify that the file has been moved, enter **cat .Desktoppolicies.txt**
 - f. Observe that the contents of the file are displayed on the screen indicating that the file was moved.
 - g. Log out of the **newuser** account.

TOPIC C

Manage User and Group Accounts

In the last topic, you created user and group accounts and even configured user profiles. Your next step will be to manage user and group accounts on an ongoing basis. This will enable you to efficiently organize your Linux environment. In this topic, you will manage user and group accounts.

Once a user or group account is created, there are many tasks that need to be performed to maintain that account. As a system administrator, you will be required to maintain the accounts and passwords of numerous users. This is achieved by effective management of user and group accounts.

The userdel Command

The `userdel` command allows you to modify the system account files, deleting all entries that refer to the login of an existing user. However, it will not allow you to remove an account if the user is currently logged in. You must kill any running processes that belong to an account before deleting the account.



Figure 2-10: The `userdel` command is used to delete an unused user account.

Syntax

The syntax of the `userdel` command is `userdel [options] {username}`.

The -r Option

The `-r` option will delete the files in the user's home directory, along with the home directory itself. Files located in other filesystems will have to be searched for and deleted manually.

The usermod Command

The `usermod` command has options that enable you to modify various user account parameters. You can change a user's name, default groups, UID, or passwords.



Figure 2-11: *The `usermod` command is used to add more information about the user.*

Some of the common `usermod` command options and their descriptions are given in the following table.

Option	Allows You To
<code>usermod -l {new login}{login}</code>	Modify the login name of the user.
<code>usermod -c "comment" login</code>	Modify the user's full name, office address, and contact numbers in the password file. Alternatively, you can use the <code>chfn {user name}</code> command to modify the details.
<code>usermod -f {number of days} {login}</code>	Modify the number of days for a password to expire and to disable the account permanently.
<code>usermod -u {new unique user ID} {login}</code>	Modify the numerical value of a user's ID, which has to be unique.
<code>usermod -d {new login directory} login</code>	Modify the user's default login directory.
<code>usermod -L {user name}</code>	Lock the password and suspend the user account temporarily.
<code>usermod -U {user name}</code>	Unlock the password.
<code>usermod -e {yyyy-mm-dd} {user name}</code>	Change the expiration date for the user account.

Syntax

The syntax of the `usermod` command is `usermod [options] {username}`.

Lock User Login

In Linux, you can lock a user's login to temporarily prevent a user from logging in to a system. This is done by disabling the user's password using the `passwd -l` command. The user's login is usually locked as a security measure, to prevent unauthorized usage when the user is unavailable.



Figure 2-12: The `passwd -l` command is used to lock the user's password.

Temporarily Suspending User Access

If you need to prevent logging in to a system through an account, but don't want to delete that account, you can edit the `/etc/shadow` file and replace the existing encrypted password with an asterisk. Be sure not to delete the colons on either side of the password because it could corrupt the file. Then, to reactivate the account, remove the asterisk and assign a new password to the user account.

Group Management

Groups, like users, are identified by a system with a unique number known as GID. In Linux, users can be members of one primary group and multiple supplemental groups. The `groupdel` and `groupmod` commands are useful in managing groups.

Command	Allows You To
<code>groupdel</code>	Delete a group from the system.
<code>groupmod</code>	Change the group's name and the numerical value of the group's ID by modifying the system account files.

Syntax

The syntax of the `groupdel` command is `groupdel {group name}`.

The syntax of the `groupmod` command is `groupmod -g {GID}`.

Group Account with GID

To add a new group to the system with a name of `print_users` and a GID of 700, enter `groupadd -g 700 print_users` at the command line.

Adding Users to a Group

As with users, the group file can be directly edited to add groups. You can use the `groupadd` command to add users instead of editing the group file.

How to Manage User and Group Accounts

Procedure Reference: Change a User's Home Directory

To change the home directory of a user:

1. Log in as root in the CLI.
2. To create a directory, enter `mkdir /{name of the directory}`.
3. To create a directory for the specified user, enter `mkdir /{name of the directory}/{user name}`.
4. To change the ownership of the directory, enter `chown {user name}[:{group name}] /{name of the directory}`.
5. To set the user's new home directory, enter `usermod -d /{name of the directory}/{user name} {user name}`.

The mkdir Command

The `mkdir` command allows you to create new directories. The syntax of the command is `mkdir {directory name}`.

The chown Command

The `chown` command is used to change the user or group that owns one or more files or directories.

Procedure Reference: Modify User Settings in the CLI

To modify user settings in the CLI:

1. Log in as root.
2. To modify user settings, enter `usermod [options] {user name}`.

Procedure Reference: Modify User Settings in the GUI

To modify user settings in the GUI:

1. Log in as root in the GUI.
2. To open the User Manager window, choose **System→Administration→Users and Groups**.
3. Modify user settings as desired.
 - To add a new user, click **Add User**.
 - To modify user settings, double-click a user name.

- To remove a user account, select the user and click **Delete**.

Procedure Reference: Remove User Accounts

To remove user accounts:

1. Log in as root.
2. To delete user accounts, enter `userdel [options] {user name}`.

Procedure Reference: Manage Default Password Aging Information

To manage default password aging information:

1. Log in as root.
2. To open the `/etc/login.defs` file, enter `gedit /etc/login.defs`.
3. Manage the password aging information.
 - To control the maximum number of days a password may be used, modify the value next to the `PASS_MAX_DAYS` variable.
 - To control the minimum number of days allowed between password changes, modify the value next to the `PASS_MIN_DAYS` variable.
 - To control the minimum password length, modify the value next to the `PASS_MIN_LEN` variable.
 - To control the number of days to issue warnings before a password expires, modify the value next to the `PASS_WARN_AGE` variable.
4. Save and close the file.

Procedure Reference: Set or Change Password Aging Information

To set or change password aging information:

1. Log in as root.
2. To change the password aging information of the specified user, enter `chage [options] {user name}`.

Procedure Reference: Modify or Delete Groups

To modify or delete groups:

1. Log in as root.
2. Manage the groups.
 - To change the GID, use the `groupmod -g {GID} {group name}` command.
 - To delete a group, use the `groupdel {group name}` command.

ACTIVITY 2-3

Configuring a New User Account

Before You Begin:

1. Log in to the CLI as root.
2. In the first terminal, modify the `/etc/skel/.bash_profile` file and remove the last line starting with `PS1`.
3. To clear the terminal screen, enter `clear`.

Scenario:

You are working as a junior system administrator, and your organization has hired a new network administrator on contract. You will need to create a user account for the new recruit based on the following details:

- User name for the new account: `netadmin1`
- Password for the `netadmin1` user: `myp$$w0rd`
- The `netadmin1` user account needs to be valid until July 2011.
- The `/home/users/netadmin1` directory should be set as the default home directory for the `netadmin1` user.

What You Do

How You Do It

- | What You Do | How You Do It |
|---|--|
| 1. Create a user account named <code>netadmin1</code> . | <ol style="list-style-type: none">a. To create a user, enter <code>useradd netadmin1</code>b. To set a password for the new user, enter <code>passwd netadmin1</code>c. To assign the password, enter <code>myp\$\$w0rd</code>d. To confirm the password, enter <code>myp\$\$w0rd</code>e. To log out of the <code>root</code> account, enter <code>logout</code> |

- | | |
|--|---|
| 2. Log in to the system using the new user account details. | a. Log in as netadmin1 .

b. To view the default home directory, enter pwd

c. Observe that /home/netadmin1 is the default home directory for the netadmin1 user.

d. Log out of the netadmin1 account. |
| <hr/> | |
| 3. Set the expiration date for the new user account. | a. Log in as root .

b. To set July 31 of the next year as the expiration date for the netadmin1 user account, enter usermod -e {year}-07-31 netadmin1 |
| <hr/> | |
| 4. Change the home directory of the netadmin1 user. | a. To create a parent directory, enter mkdir /home/users

b. To create a home directory, enter mkdir /home/users/netadmin1

c. To change the ownership of the directory, enter chown netadmin1:netadmin1 /home/users/netadmin1

d. To change the default home directory of the netadmin1 user to /home/users/netadmin1 , enter usermod -d /home/users/netadmin1 netadmin1

e. Log out of the root account. |
| <hr/> | |
| 5. Check that the home directory of the netadmin1 user has changed. | a. Log in as netadmin1 .

b. To view the new home directory, enter pwd

c. Observe that the home directory has changed to /home/users/netadmin1 .

d. Log out of the netadmin1 account. |
-
-

ACTIVITY 2-4

Managing Group Accounts

Before You Begin:

- 1. Log in to the CLI as root.
- 2. On the terminal, create two groups named Finance and Marketing.
- 3. To clear the terminal screen, enter `clear`.

Scenario:

You are assigned the task of changing the GID for the finance department so that it matches the department number. In addition, you need to remove the marketing group from the system because the work of the marketing department will be outsourced to another company from now on.

What You Do	How You Do It
1. Change the GID to match the finance department number, 555.	<ul style="list-style-type: none">a. To alter the GID of the finance department, enter <code>groupmod -g 555 Finance</code>b. To verify that the change was made, enter <code>tail -20 /etc/group</code>c. Observe that the GID of the finance department has been changed.
2. Delete the user group, Marketing.	<ul style="list-style-type: none">a. Enter <code>groupdel Marketing</code>b. To verify that the Marketing group was deleted, enter <code>cat /etc/group less</code>c. To verify that the Marketing group is no longer listed, press the Spacebar till you reach the end of the file.d. To quit the display, press <code>Q</code>.e. Clear the terminal screen.

Lesson 2 Follow-up

In this lesson, you created and managed user and group accounts. This will help you efficiently organize and maintain a Linux environment with numerous users.

1. How is organizing users into groups useful to you?
2. Why is it essential to configure a user profile?

LESSON 3

Managing Partitions and the Linux Filesystem

Lesson Time

2 hour(s), 30 minutes

In this lesson, you will manage partitions and the Linux filesystem.

You will:

- Create partitions.
- Navigate through the Linux filesystem.
- Manage the Linux filesystem.
- Maintain the Linux filesystem.

Introduction

You are now familiar with user and group accounts in Linux. Further, you need to manage the Linux filesystem. In this lesson, you will create partitions on the hard disk and navigate, manage, and maintain the Linux filesystem.

Data organization facilitates efficient resource management and faster retrieval of information. Data organization is done by sorting data into filesystems. The Linux filesystem is part of what sets Linux apart from other operating systems. Understanding the structure and workings of the filesystem will assist you in storage, management, and troubleshooting of data.

This lesson covers all or part of the following CompTIA Linux+ Powered by LPI certification objectives:

- Topic A:
 - Objective 102.1, Objective 104.1, Objective 104.2, Objective 104.3, Objective 104.7
- Topic B:
 - Objective 101.1, Objective 102.1, Objective 102.3, Objective 103.1, Objective 103.3, Objective 104.3, Objective 104.7
- Topic C:
 - Objective 102.1, Objective 104.1, Objective 104.3
- Topic D:
 - Objective 101.1, Objective 104.2

TOPIC A

Create Partitions

Before you work with the Linux filesystems, you should partition the hard disk of your system. Proper partitioning of the hard disk will ensure that users have enough space to store their data. In this topic, you will create and manage disk partitions.

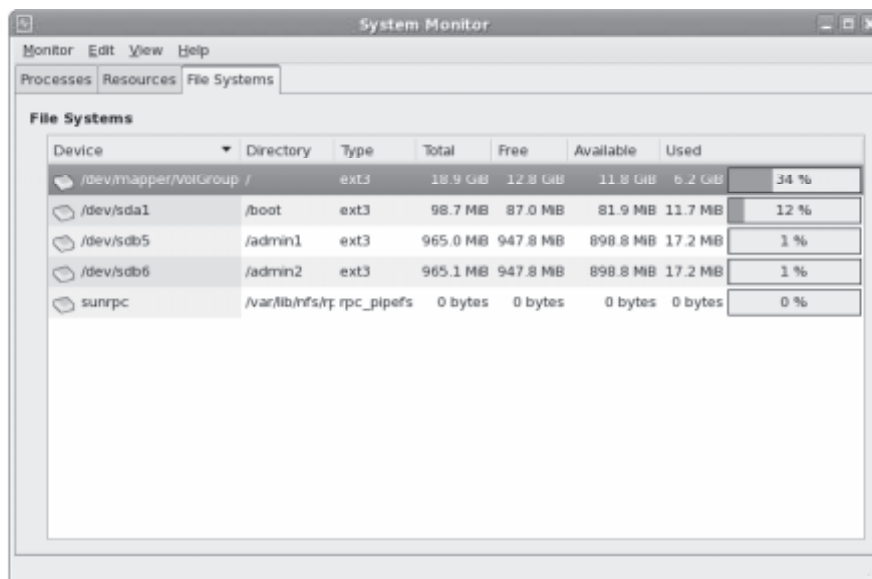
The hard disk is the most critical component for data storage in any system. Without effective disk partitioning, data on the disk will be unorganized and cluttered, or the users might run out of available storage space prematurely. Improper disk partitioning may also contribute to a system crash. As a Linux administrator, it is your responsibility to ensure that disks are partitioned properly such that users have enough space to store their data in an efficient manner.

Filesystems

Definition:

A *filesystem* is a method that is used by an operating system to store, retrieve, organize, and manage files and directories on mass storage devices. A filesystem maintains information, such as the date of creation and modification of individual files, their file size, file type, and permissions, and it provides a structured form for data storage. A filesystem by itself does not interpret the data contained in files because this task is handled by specific applications. Filesystems vary depending on several parameters, such as the purpose of the filesystems, the information they store about individual files, the way they store data, and data security.

Example:



Device	Directory	Type	Total	Free	Available	Used
/dev/mapper/volGroup /		ext3	18.9 GiB	12.8 GiB	11.8 GiB	6.2 GiB 34 %
/dev/sda1	/boot	ext3	98.7 MiB	87.0 MiB	81.9 MiB	11.7 MiB 12 %
/dev/sdb5	/admin1	ext3	965.0 MiB	947.8 MiB	898.8 MiB	17.2 MiB 1 %
/dev/sdb6	/admin2	ext3	965.1 MiB	947.8 MiB	898.8 MiB	17.2 MiB 1 %
sunrpc	/var/lib/dfs/rp/rpc_pipefs		0 bytes	0 bytes	0 bytes	0 bytes 0 %

Figure 3-1: Files are stored in directories.

Filesystem Labels

Filesystem labels are assigned to filesystems for easy identification. The labels may be up to 16 characters long and can be displayed or changed using the `e2label` command.



Figure 3-2: An example of a filesystem label.

Syntax

The syntax for setting filesystem labels is `e2label /dev/{device name}{partition number} {label name}`. They can also be set using the `tune2fs -L {volume label} {device}` command.

Filesystem Types

Linux supports many common filesystem types. Some common filesystem types are described in the following table.

Filesystem Type	Description
ext2	This used to be the native Linux filesystem of some of the previous releases. It is still supported in the current releases of Linux.
ext3	This is an improved version of ext2. In case of an abrupt system shutdown, ext3 is much faster in recovering data and better ensures data integrity. You can easily upgrade your filesystem from ext2 to ext3.
ext4	The newest default filesystem for Linux distributions. It is backwards-compatible with the ext2 and ext3 filesystems. Among ext4's improvements over ext3 are journaling, support of volumes of up to one exbibyte (EiB) and files up to 16 tebibytes (TiB) in size.

Filesystem Type	Description
reiserfs	This can handle small files efficiently. It handles files smaller than 1K and is faster than ext2. If appropriately configured, it can store more data than ext2.
vfat	This is a 32-bit filesystem and supports long file names. It is compatible with the FAT filesystem of Microsoft Windows XP and Microsoft Windows NT.
XFS	This is a 64-bit, high-performance journaling filesystem that provides fast recovery and can handle large files efficiently.
JFS	This is a 64-bit journaling filesystem that is fast and reliable. It is better equipped to handle power failures and system crashes.
swap	This is not a true filesystem, but rather is a portion of the hard disk that is used in situations when Linux runs out of physical memory and needs more of it. Linux pushes some of the unused files from RAM to “swap” to free up memory.
ISO 9660	This is a filesystem standard defined by the International Organization for Standardization (ISO), and is also called a CDFS (Compact Disc File System). Linux allows you to access DVDs and CDs that use this filesystem.

Access Other Filesystems

Linux allows you to access other filesystems and mount them when required. However, you cannot install Linux on these filesystems.

Filesystem	Description
FAT	The FAT (File Allocation Table) filesystem is compatible with different operating systems, including all versions of Windows, MS-DOS, and UNIX. It is primarily used for formatting floppy disks.
NTFS	NTFS (New Technology File System) is the recommended filesystem for Windows-based computers. NTFS provides many enhanced features over FAT or vfat, including file- and folder-level security, file encryption, disk compression, and scalability to very large drives and files.

Partitions

Definition:

A *partition* is a section of the hard disk that logically acts as a separate disk. Partitions enable you to convert a large hard disk to smaller manageable chunks, leading to better organization of information. A partition must be formatted and assigned a filesystem before data can be stored on it. Partitions are identified using a partition table, which is stored in the boot record. The partition table can contain entries for a maximum of four primary partitions. Partitions can be classified into primary and extended partitions. The size of each partition can vary but cannot exceed the total free space of the hard disk.

Example:

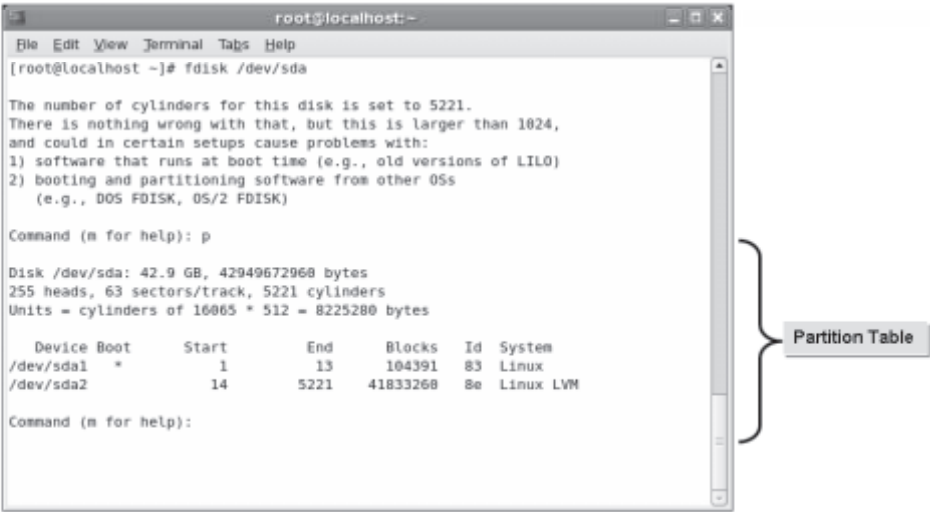


Figure 3-3: Partitions on a hard disk.

Hard Disk Size Specification

Before proceeding with the installation process, you need to plan the hard disk layout based on your requirements. Each partition has a recommended size specification. The following table lists the recommended size specification for partitions.

Partition	Recommended Size
/	Minimum 1 GB.
/boot	100 MB.
swap	Double the RAM size.
/var	Minimum 250 MB. If the possibility of the installation of many applications exists in the future, allocate the appropriate size.
/home	Varies based on the number of users.

Disk Partitioning

Most operating systems, including Linux, use disk partitions. Data of different types can be stored in separate locations on the hard disk. The partition size can be specified by a user. However, the filesystem size must be considered before specifying the partition size. Disk partitioning enables the user to separate system files from user accessible ones. Corrupted partitions do not affect the other partitions, and they can be recovered separately.

Partition Types

There are three types of partitions: primary, extended, and logical. The functionality of the hard disk depends on the types of partitions on it.

Each partition has a set of specific features. The three types of partitions are described in the table.

Partition Type	Description
<i>Primary</i>	A disk partition that can contain one filesystem or logical drive and is sometimes referred to as volumes. A maximum of four primary partitions are allowed. The swap filesystem and the boot partition are normally created in a primary partition.
<i>Extended</i>	An extended partition can contain several filesystems, which are referred to as logical disks or logical drives. There can be only one extended partition, which can be further subdivided. This partition type does not contain any data and has a separate partition table.
<i>Logical</i>	A part of a physical disk drive that has been partitioned and allocated as an independent unit and functions as a separate drive. A logical partition is created within an extended partition. There is no restriction on the number of logical partitions, but it is advisable to limit it to 12 logical partitions per disk drive.

The fdisk Utility

fdisk is a menu-driven utility program that is used for creating, modifying, or deleting partitions on a disk drive. Using *fdisk*, a new partition table can be created, or existing entries in the partition table can be modified. The *fdisk* utility understands the DOS and Linux type partition tables. Depending on the partition table created, the DOS FDISK or the Linux *fdisk* program is invoked. The *fdisk* utility also allows you to specify the size of partitions.

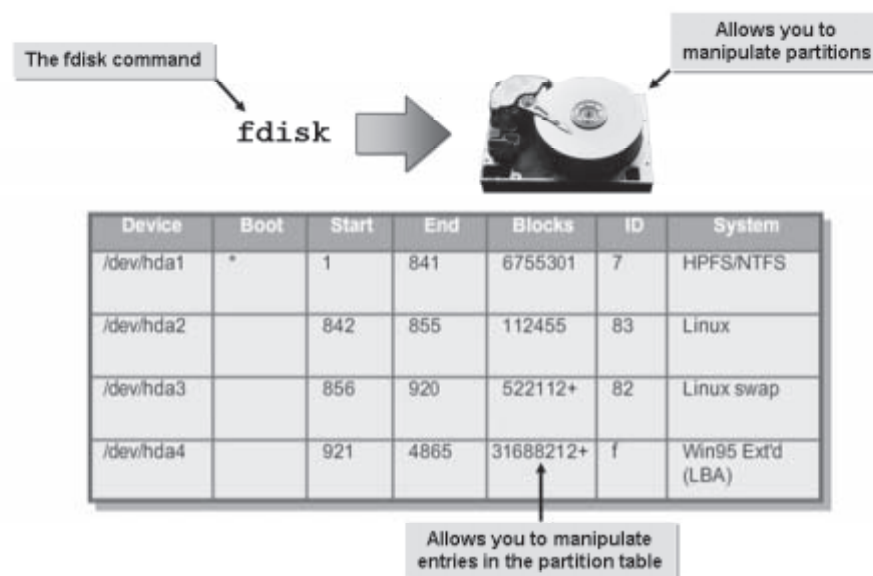


Figure 3-4: A partition table created with the `fdisk` utility.

Syntax

The syntax of the `fdisk` utility is `fdisk [options] {device name}`.

Command Line Options Supported by `fdisk`

The `fdisk` utility supports a number of command line options.

Option	Enables You To
<code>-b sector size</code>	Specify the number of disk sectors.
<code>-H heads</code>	Specify the number of disk heads.
<code>-S sectors</code>	Specify the number of sectors per track.
<code>-s partition</code>	Print the partition size in blocks.
<code>-v</code>	List the <code>fdisk</code> version.
<code>-l</code>	List partition tables for devices.

`fdisk` Utility Options

The `fdisk` utility provides various options for partitioning disks according to the requirements of users.

Some of the `fdisk` options are described in the following table.

Option	Enables You To
<code>n</code>	Create a new partition. The sub-options allow you specify the partition type and partition size.
<code>d</code>	Remove a partition.

Option	Enables You To
p	List the existing partitions.
w	Write the changes to the disk and exit the utility.
q	Cancel the changes made and exit the utility.

The fstab File

The *fstab* file is a configuration file that stores information about storage devices and partitions and where and how the partitions should be mounted. The *fstab* file is located in the */etc* directory. It can be edited only by a root user. The *fstab* file consists of a number of lines—one for each filesystem.

Each line in an *fstab* file has six fields, which are separated by spaces.

Field	Description
Device or partition name	Specifies the name of the device or filesystem that has to be mounted.
Default mount point	Indicates where the filesystem has to be mounted.
Filesystem type	Specifies the type of filesystem used by the device or partition.
Mount options	Specifies a set of comma-separated options that will be activated when the filesystem is mounted.
Dump options	Indicates if the <i>dump</i> utility should back up the filesystem. Usually, zero is specified as the <i>dump</i> option to indicate that <i>dump</i> can ignore the filesystem.
fsck options	Specifies the order in which the <i>fsck</i> utility should check filesystems.

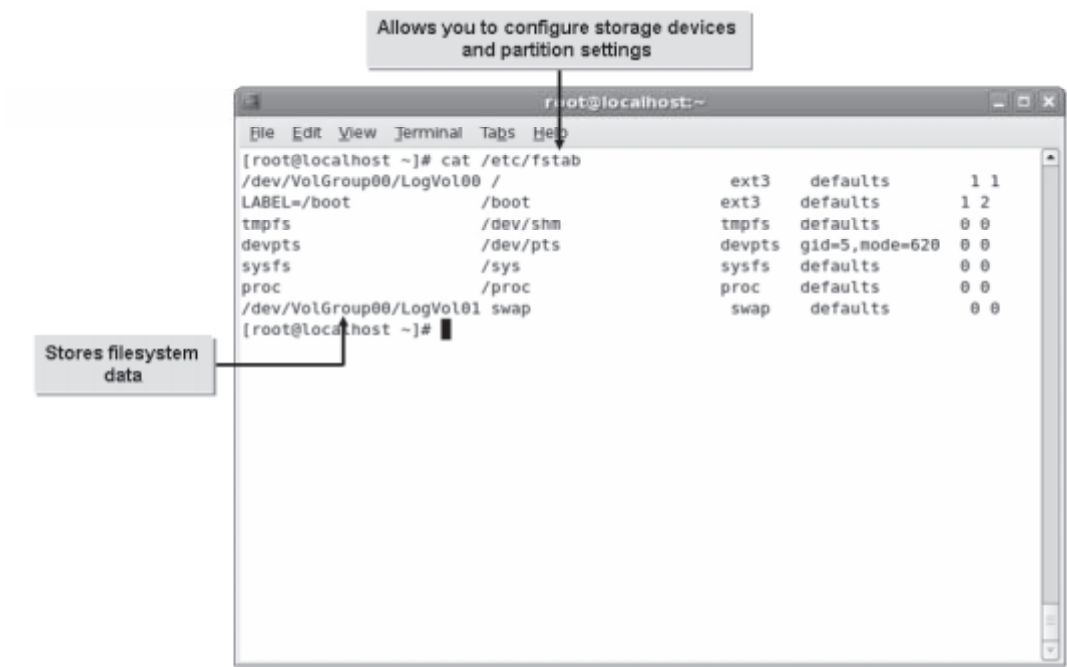


Figure 3-5: The `/etc/fstab` file contains partition and filesystem settings.

The mkfs Command

The `mkfs` command is used to build a Linux filesystem on a device, which is usually a hard disk partition. The following table lists some options of the `mkfs` command and their description.

Option	Allows You To
<code>-v</code>	Produce <i>verbose</i> output, where the output message will keep changing constantly as the program is processing.
<code>-V</code>	Produce verbose output, including all filesystem-specific commands that are executed.
<code>-t {fstype}</code>	Specify the type of filesystem to be built.
<code>fs-options</code>	Pass filesystem-specific options to the filesystem builder.
<code>-c</code>	Check the device for bad blocks before building the filesystem.
<code>-l {file name}</code>	Read the list of bad blocks from a specified file.

Building New Linux Filesystems Using the mkfs Commands

The `mkfs` commands are used to build a new Linux filesystem. The different `mkfs` commands are given in the following table.

If You Need To Build	Use This <code>mkfs</code> Command
An ext2 filesystem	<code>mkfs.ext2 /dev/hdaPartition number</code>

If You Need To Build	Use This <code>mkfs</code> Command
An ext3 filesystem	<code>mkfs.ext3 /dev/hdaPartition number</code>
An ext4 filesystem	<code>mkfs.ext4 /dev/hdaPartition number</code>
A reiserfs filesystem	<code>mkfs.reiserfs /dev/hdaPartition number</code>
A vfat filesystem	<code>mkfs.vfat /dev/hdaPartition number</code>
An XFS filesystem	<code>mkfs.xfs /dev/hdaPartition number</code>
A JFS filesystem	<code>mkfs.jfs /dev/hdaPartition number</code>

Syntax

The syntax of the `mkfs` command is `mkfs [filesystem type] [options] {device}`.


The `mke2fs` Utility

The `mke2fs` utility is used to create ext2, ext3, and ext4 filesystems, and it has various options. Some of the options are listed below in the following table.

Option	Enables You To
<code>-b {block size}</code>	Specify the size of the block in bytes.
<code>-c</code>	Check the device for errors in the blocks, before creating the filesystem.
<code>-f</code>	Specify the fragment size in bytes.
<code>-j</code>	Create a journaled ext3 filesystem.
<code>-M</code>	Set the directory that was last accessed for the filesystem to be mounted.
<code>-V</code>	Print the version number of the <code>mke2fs</code> utility.

Syntax

The syntax of the `mke2fs` utility is `mke2fs [options] {device}`.

 The command `mke2fs /dev/hdaPartition number` will allow you to build an ext2 filesystem.

Device Recognition by the MBR

Device recognition is performed by the MBR at system startup, by recognizing the hard disk and all the partitions on it. The MBR has two main components that help it to detect any devices that are connected to the system.

Component	Description
The Master Partition Table	Contains the list of partitions on the hard disk. Technically, the hard disk can have many partitions. The table displays the partition id, its starting cylinder, and the number of cylinders occupied by the partition.
The Master Boot Code	Contains the program for loading the operating system on the hard disk. This program is loaded to initiate the boot process.

The Cylinder

The *cylinder* is the aggregate of all tracks that reside in the same location on every disk surface. On multiple-platter disks, the cylinder is the sum total of every track with the same track number on every surface. On a hard disk, a cylinder comprises the top and corresponding bottom tracks.

Partition Management

Partition management is the process of creating, destroying, and manipulating partitions to optimize system performance. Effective partition management enables you to keep track of the data in the partitions and avoid data overflow. Various utilities, such as `sfdisk`, `partprobe`, and GNU `parted`, are available for partition management.

The sfdisk Utility

The *sfdisk* utility is used to manipulate partitions. This utility manages partitions by listing the number of partitions and their sizes, checking the partitions, and repartitioning a storage device.

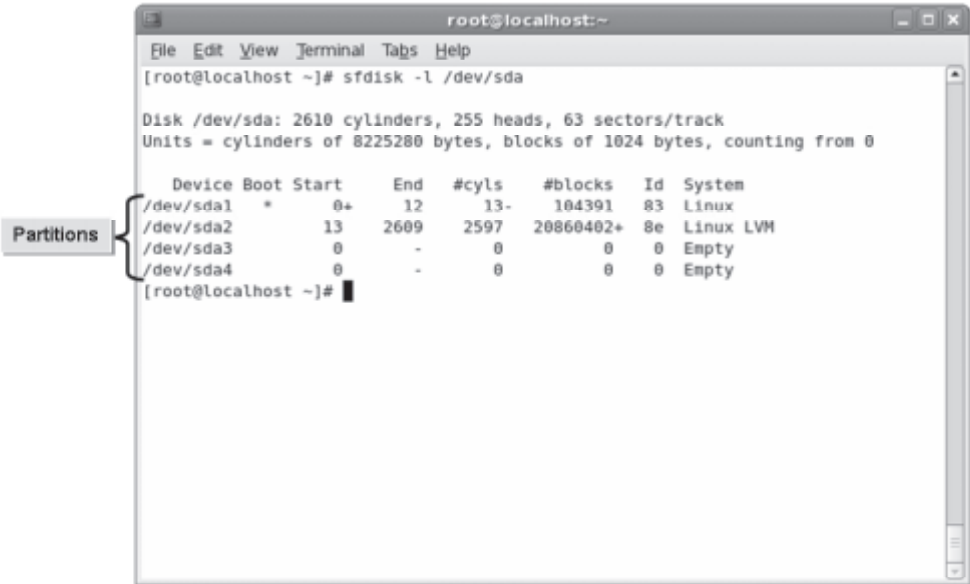


Figure 3-6: Listing partitions on the hard disk using the `sfdisk` utility.

Various options are available in the `sfdisk` utility to manage partitions.

Option	Enables You To
-s	List the partition size.
-l {device}	List partitions on all hard disks.
-V {device}	Check for consistency in all partitions.
device	Repartition hard disks. However, if the code is wrongly entered, it may lead to loss of data.
-i	Increment numbers starting with 1 instead of 0 for all cylinders in the hard disk.
-A {number}	Activate the partition indicated by the partition number while making all other partitions inactive.

Syntax

The syntax of the `sfdisk` utility is `sfdisk [options] device`.

The GNU Parted Utility

The *GNU Parted* utility is also used to manage partitions. It is particularly useful when creating partitions on new hard disks. It can be used to create, destroy, and resize partitions. This utility is generally not used for resizing ext3 partitions.



Figure 3-7: The welcome screen of the GNU Parted utility.

A number of options are available in the GNU Parted utility.

Option	Enables You To
-h	Display a help message.
-v	Display the version of GNU Parted.

Option	Enables You To
-i	Configure parted to ask for user input.
-s	Stop parted from asking for user input.

Syntax

The syntax of the parted utility is `parted [option] device {command [argument]}`.

The partprobe Program

The *partprobe* program is used to update the kernel with changes in the partition tables. The program first checks the partition table and if there are any changes it automatically updates the kernel with the changes.



Figure 3-8: Using the *partprobe* utility to display the storage devices and their partitions.

The *partprobe* program has several options.

Option	Enables You To
-d	Cancel any updates.
-s	Display the storage devices and their partitions.
-v	Display the version of the partprobe program.

Syntax

The syntax of the partprobe utility is `partprobe [options] [device]`.

How to Create Partitions

Procedure Reference: Create a Primary Partition

To create a primary partition:

1. Log in as root.
2. To partition the disk, enter `fdisk /dev/{device name}`.
3. To create a partition, enter `n`.
4. Create a primary partition.
 - a. To create a primary partition, enter `p`.
 - b. To accept the default starting point of the partition, press **Enter**.
 - c. Specify the partition size.
 - To accept the default partition size, press **Enter**.
 - To specify a custom partition size.
 - To specify the partition size in blocks, enter `+[Required size]`.
 - To specify the partition size in kilobytes (KB), enter `+[Required size]K`.
 - To specify the partition size in megabytes (MB), enter `+[Required size]M`.
5. To write the partition table on the disk and exit the utility, enter `w`.
6. To update the partition table, enter `partprobe` or reboot the system.
7. To list the partition table, enter `sfdisk -l /dev/{device name}`.

Procedure Reference: Create an Extended Partition

To create an extended partition:

1. Log in as root.
2. To begin disk partitioning, enter `fdisk /dev/{device name}`.
3. To create a partition, enter `n`.
4. Create an extended partition.
 - a. To create an extended partition, enter `e`.
 - b. To accept the default starting point of the partition, press **Enter**.
 - c. To accept the default partition size, press **Enter**.
 - d. To create a logical partition within the extended partition, enter `n`.
 - e. To accept the default starting point of the partition, press **Enter**.
 - f. Specify the partition size.
 - To accept the default partition size, press **Enter**.
 - To specify a custom partition size.
 - To specify the partition size in blocks, enter `+[Required size]`.
 - To specify the partition size in kilobytes (KB), enter `+[Required size]K`.

- To specify the partition size in megabytes (MB), enter **+[Required size]M**.
5. To write the partition table on the disk and exit the utility, enter `w`.
 6. To update the partition table, enter `partprobe` or reboot the system.
 7. To list the partition table, enter `sfdisk -l /dev/{device name}`.

Procedure Reference: Apply Labels to a Partition

To apply labels to a partition:

1. Log in as root.
2. To apply a label to the partition, at the command prompt, enter `e2label /dev/{device name}{partition number} {label name}`.
3. To view the applied or associated label, enter `e2label /dev/{device name}{partition number}`.
4. If necessary, to mount the partition using its label, enter `mount LABEL = {label name} {mount point}`.

ACTIVITY 3-1

Creating Partitions

Before You Begin:

1. On `srvA`, you have logged in to the CLI as root.
2. To create two directories, at the command line, enter `mkdir /morning /evening`
3. Clear the terminal screen.

Scenario:

Your organization has a support team that works in two shifts. One employee uses a system in the morning shift and the same system is used by another in the evening shift. Both need to have separate partitions mounted according to the details given here:

- The logical partitions, `sdb5` and `sdb6`, need to be mounted on `/morning` and `/evening` directories, respectively.
- Login name for the root user: `root`
- Password for the root user: `p@ssw0rd`

You also need to ensure that these partitions are easily identified for maintenance. The labels that need to be applied to the partitions and used for mounting them are:

- For the morning shift: `Mrng`
- For the evening shift: `Evng`

What You Do	How You Do It
1. Create an extended partition.	<ol style="list-style-type: none"> To begin the disk partitioning process, enter fdisk /dev/sdb To create a new partition, enter n To create an extended partition, enter e To accept the default starting point of the partition, press Enter. To specify the size of the partition, enter +15000M
2. Create two logical partitions within the extended partition.	<ol style="list-style-type: none"> To create a new partition, enter n To accept the default starting point of the partition, press Enter. To specify the size of the partition, enter +1024M To create another logical partition of size 1024M, repeat the steps from (a) to (c). To write the partition table on the disk and exit the utility, enter w To restart the system, enter reboot At the GUI Login screen, press Ctrl+Alt+F1 to switch to the first terminal. Log in as root in the CLI with the password as p@ssw0rd
3. Set logical partitions for the ext2 filesystem.	<ol style="list-style-type: none"> To create an ext2 filesystem on /dev/sdb5, enter mkfs.ext2 /dev/sdb5 To clear the terminal screen, enter clear To create an ext2 filesystem on /dev/sdb6, enter mkfs.ext2 /dev/sdb6 To clear the terminal screen, enter clear

LESSON 3

4. Verify that the two new partitions have the ext2 filesystem.
 - a. To run the GNU Parted utility, enter **parted**
 - b. To select the sdb partition, enter **select /dev/sdb**
 - c. To view the list of existing partitions, at the **(parted)** prompt, enter **print**
 - d. Observe that the partitions five and six have the **ext2** filesystem.
 - e. To quit from the parted utility, enter **q**
 - f. To clear the terminal screen, enter **clear**

5. Apply labels to the partition.
 - a. To view the existing label of the /dev/sdb5 partition, enter **e2label /dev/sdb5**
 - b. Observe that there is no label set for the /dev/sdb5 partition.
 - c. To apply a new label **Mrng** to the partition, enter **e2label /dev/sdb5 Mrng**
 - d. To view the existing label of the /dev/sdb6 partition, enter **e2label /dev/sdb6**
 - e. Observe that there is no label set for the /dev/sdb6 partition.
 - f. To apply a new label **Evng** to the partition, enter **e2label /dev/sdb6 Evng**
 - g. To clear the terminal screen, enter **clear**

6. Verify the labels applied to the partitions.
 - a. To verify that the partition label for `/dev/sdb5` has changed, enter **e2label /dev/sdb5**
 - b. Observe that the label is set as "Mrng" for the `/dev/sdb5` partition.
 - c. To verify that the partition label for `/dev/sdb6` has changed, enter **e2label /dev/sdb6**
 - d. Observe that the label is set as "Evng" for the `/dev/sdb6` partition.

7. Mount the partitions using their labels.
 - a. To mount the `/dev/sdb5` partition using its label, enter **mount LABEL=Mrng /morning**
 - b. To mount the `/dev/sdb6` partition using its label, enter **mount LABEL=Evng /evening**
 - c. To verify that the partitions have been mounted using their labels, enter **mount**
 - d. Observe that the partitions `/dev/sdb5` and `/dev/sdb6` are mounted on `/morning` and `/evening` directories.
 - e. To clear the terminal screen, enter **clear**

TOPIC B

Navigate Through the Linux Filesystem

Now that you partitioned your hard disk properly and efficiently, it is time to move around the Linux filesystem. In this topic, you will navigate through the filesystem.

Navigating through the Linux filesystem will allow you to access, create, and delete files and directories. While being able to navigate through the filesystem in the GUI environment may be easier, the CLI will give you more direct control over the workings of the Linux system.

Filesystem Hierarchy

Linux comprises regular files that include text files, executable files or programs, input for programs, and output from programs. Besides these, the Linux filesystem consists of other types of files.

These file types are described in the following table.

File Type	Description
Directories (d)	Contains the lists of all files.
Special files	Includes system files. These files are in the /dev format. These can be <i>block special files</i> (b) or <i>character special files</i> (c). Block special files are large files that are used for data storage. Character special files are small files that are used for streaming of data.
Links (l)	Makes a file accessible in multiple parts of the system's file tree.
Domain sockets (s)	Provides inter-process networking that is protected by the filesystem's access control.
Named pipes (p)	Allows processes to communicate with each other, without using network sockets.

The file Command

The `file` command is used to determine the type of file. The syntax of the command is `file [options] {file name}`.

The FHS

The *Filesystem Hierarchy Standard (FHS)* is a collaborative document that specifies a set of guidelines for the names of files and directories and their locations. The important advantages of implementing the guidelines of the FHS include compatibility between the systems that are FHS compliant and restriction on users changing the /usr partition that contains common executable files.



The restriction on users to prevent changes to the /usr partition is achieved by mounting /usr as a read-only partition.




The complete documentation of FHS is available at <http://www.pathname.com/fhs/>.


Standard Directories

The Linux operating system comprises directories that enable you to organize user files, drivers, logs, programs, and utilities into different categories. In Linux, a forward slash (/) represents the root directory, which is the topmost directory, and all other directories are subdirectories under it.

Some of the standard root directories are described in the following table.

Directory	Description
/boot	Stores the files necessary to boot the Linux operating system. The /boot partition must be present in the first sector of the hard disk, from which the system boots. For example, the /boot/grub/menu.lst file.
/bin	Stores essential command line utilities and binaries. For example, the /bin/lis file.
/dev	Stores hardware and software device drivers. It maintains filesystem entries that represent the devices connected to the system. For example, the /dev/sda1 driver.
/etc	Stores basic configuration files. For example, the /etc/samba/smb.conf file.
/lib	Stores shared program libraries required by the kernel, command line utilities, and binaries. For example, the /lib/libc.so.6 file.
/sbin	Stores binaries that are used for completing the booting process and also the ones that are used by the root user—the administrator. For example, the /sbin/ifconfig file.
/usr	Stores small programs and files accessible to all users. For example, the /usr/share/doc file.
/var	Stores system log files, printer spools, and some networking services' configuration files. For example, the /var/log/messages file.
/tmp	Stores temporary files. For example, the /tmp/filename.tmp file.
/opt	Stores files of large software packages. These packages normally create a subdirectory bearing their name under the /opt directory and then place their files in the subdirectory. For example, the /opt/nessus file.
/mnt	Is the mount point for temporarily mounting data from locations such as floppy disks, CDs, DVDs, and network partitions.
/media	Allows access to temporary and removable filesystems such as CD-ROMs and floppy disks.

 In Linux, every user, except the root user, is assigned a specific directory by default in /home to work. Users can then create subdirectories and files within this directory. As soon as the users log in to the system, their own control is automatically placed in their home directory. The home directory of the root user is /root.

 Based on your need, allocate disk space to each directory in the FHS. For example, when connected to a network with more than a hundred users, you can allocate more disk space to the /home directory so that users each can be allotted more storage space on their home directory.

/usr Subdirectories

The /usr directory contains some important subdirectories.

Subdirectory	Description
/usr/bin	Includes executable programs that can be executed by all users.
/usr/local	Includes custom build applications that are stored here by default.
/usr/lib	Includes object libraries and internal binaries that are needed by the executable programs.
/usr/lib64	Serves the same purpose as /usr/lib, except that it is meant only for 64-bit systems.
/usr/share	Includes read-only architecture independent files. These files can be shared among different architectures of an operating system.

File Naming Conventions

A file name is a string of characters that identify a file. By using the right combination of characters in file names, you can ensure that the files are unique and easy to recognize.

Guidelines:

Creating File Names with Space

You can create file names with spaces between characters by including a backward slash (\) along with a space in the file name. For example: `touch Audit\`
`File.txt` will create a file named Audit File.txt.

File Browsers

In Linux, you can navigate through a filesystem using a file browser. The default file browser on GNOME desktops in Red Hat and Fedora distributions is the Nautilus browser. This browser operates in two modes.

Mode	Description
<i>Spatial</i>	This is the default mode that enables you to open a particular window at exactly the same position on the screen by remembering the last position. Each folder or directory that you select is opened in a new browser window.
<i>Browser</i>	This is the mode that enables you to display the selected folder in the same window. You need to modify the preferences in the Computer window.



Figure 3-9: *The Nautilus file browser.*

The Home Directory

The *home directory* is where you are placed when you log in to the system. In Linux, by default, every user, except the root user, is assigned a specific directory in `/home`. In many shells, including Korn, C shell, and Bash, the tilde character (`~`) represents your home directory. A user can create subdirectories and files within this directory. As soon as the user logs in to the system, control is automatically transferred to the user's home directory. The home directory of the *root user* is `/root`. The root user can access all files and resources on the system.

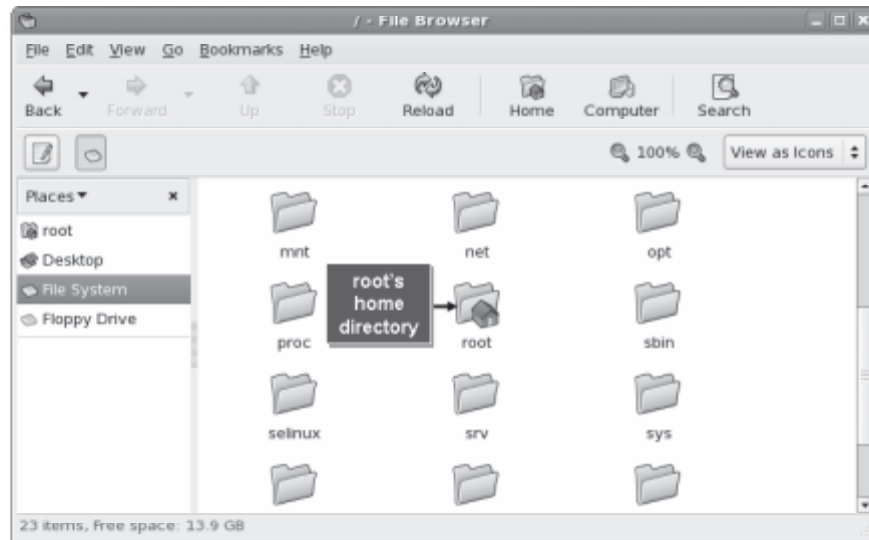


Figure 3-10: The home directory of the root user.

The Current Working Directory

The *current working directory* is the location on the system that you are accessing at any point in time. For example, when you log in to a system, you are placed in your home directory. So, your current working directory is your home directory. The current working directory can be listed in shorthand with a period (`.`).

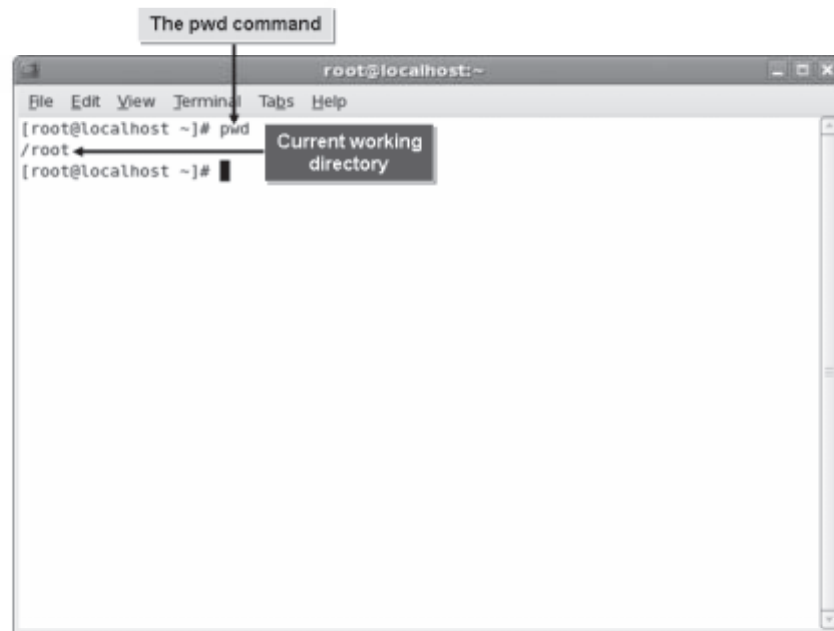


Figure 3-11: Viewing the current working directory using the `pwd` command.

The `pwd` Command

When you navigate through a filesystem, you may need to know your current working directory. The `pwd` command displays your current working directory relative to the root directory. It displays the full path name.

The Parent Directory

The *parent directory* is one level above your current working directory. All directories, except the root directory, have a parent directory. You can use the double period notation to switch to the parent directory.

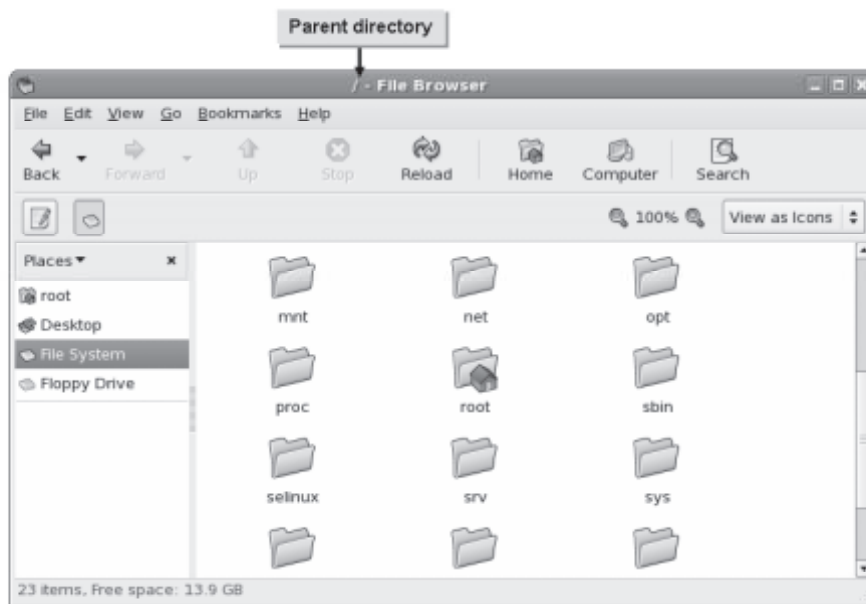


Figure 3-12: The root (/) directory is the parent directory for all other directories.

Paths

Definition:

A *path* specifies a location in the filesystem. It begins with the root directory, the directory at the top of the directory tree, and ends with the directory or file you want to access.

You can refer to a particular file by providing a path to the specific directory that contains the file. For example, the directory jsmith contains a subdirectory, work, which contains a file named mywork. To refer to that file, use the following path name: /home/jsmith/work/mywork. Notice that the forward slash (/) character is used to separate items in the path. The slash that precedes jsmith represents the root directory, from which the path to the file, mywork, begins.

Example:

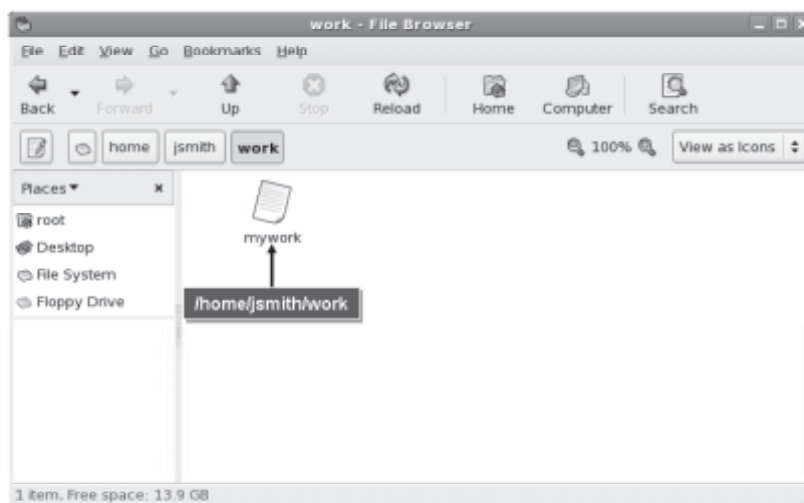


Figure 3-13: The path to the file mywork.

Absolute and Relative Paths

Paths are of two types—absolute and relative. *Absolute path* refers to the specific location, including the domain name, irrespective of the current working directory or combined paths. These paths are usually written with reference to the root directory, and therefore start with a forward slash. Paths that do not begin with a forward slash are called relative paths. A *relative path* is the path relative to the current working directory; therefore, the full absolute path need not be included. These paths can contain the period [.] and double period [. .], which are indications for the current and parent directories.



Figure 3-14: Listing files in a directory using the absolute path.

Basic Filesystem Commands

There are some basic filesystem commands that will allow you to modify files and display information within the Linux filesystem.

Command	Enables You To
<code>cd</code>	Traverse the directory structure. There are several ways to specify the path name of the directory you need to switch to. The syntax of the <code>cd</code> command is <code>cd {absolute or relative path}</code> .
<code>ls</code>	List the files in the current working directory. This command displays only the file name when the command is run without any options. However, it can be used to list information such as size, file type, and permissions by running the command with the respective options. The syntax of the <code>ls</code> command is <code>ls [options] [absolute or relative path of the directory]</code> .
<code>mv</code>	Move files and directories from one directory to another, or renames a file or directory. The syntax of the <code>mv</code> command is <code>mv {absolute or relative path}/{file or directory name} {absolute or relative path}/{new file or directory name}</code> .
<code>cp</code>	Copy a file. The syntax of the <code>cp</code> command is <code>cp [options] {absolute or relative path of the file or directory to be copied}/{file or directory name} {absolute or relative path of the destination}</code> . You can use the <code>-R</code> option of the <code>cp</code> command to copy files along with the source directory recursively. The syntax is: <code>cp -R {source directory}/{target directory}</code> .
<code>rm</code>	Delete files or directories. The syntax of the <code>rm</code> command is <code>rm [options] {absolute or relative path of file or directory}/{file or directory name}</code> . You can use the <code>-R</code> option of the <code>rm</code> command to recursively remove files, subdirectories, and the directory itself. The syntax is: <code>rm -R {directory and content that needs to be deleted}</code> .
<code>touch</code>	Change the time of access or modification time of a file to the current time. In addition, the <code>touch</code> command creates an empty file if the file name specified as an argument does not exist. The syntax of the <code>touch</code> command is <code>touch {file name}</code> .
<code>mkdir</code>	Create a directory. The syntax of the <code>mkdir</code> command is <code>mkdir {directory name}</code> .
<code>rmdir</code>	Delete directories. The syntax of the <code>rmdir</code> command is <code>rmdir {directory name}</code> .
<code>pushd</code>	Add a directory at the top of a stack of directories or rotate a stack of directories. The syntax of the <code>pushd</code> command is <code>pushd [options] {directory name}</code> .

Command	Enables You To
<code>popd</code>	Remove entries from a stack of directories. When no option is specified, it removes the top directory from the stack. The syntax of the <code>popd</code> command is <code>popd [options]</code> .

The -v Option

`-v` is a command option that can be used with the basic file management commands. This option explains the running of the command to produce the desired output, in a verbose manner.

The ls Command Options

The `ls` command options are described in the following table.

Option	Description
<code>-l</code>	Displays a long list including the permissions, number of hard links, owner, group, size, date, and file name.
<code>-F</code>	Displays the nature of a file, such as <code>*</code> for an executable file and <code>/</code> for a directory.
<code>-a</code>	Displays all files present in the directory, including the files whose names begin with a period (<code>.</code>).
<code>-R</code>	Recursively displays all subdirectories.
<code>-d</code>	Displays information about symbolic links or directories rather than the link's target or the contents of the directory.
<code>-L</code>	Displays all files in a directory including symbolic links.

Changing the Current Directory

There are times when you need to move out of your home directory into another directory in the filesystem. In such situations, you can use the `cd` command to change directories. The `cd` command enables you to traverse the directory structure. There are several ways to specify the path name to the directory that you wish to make your working directory:

- The `cd` command without a path name takes you to your home directory, irrespective of your current directory.
- The `cd [path name]` command takes you to the path name specified. The path name can be the full path name (from the root down to the specified directory) or the relative path name (starting from your current working directory).
- The `cd ~/ [path name]` command takes you to the specified directory, relative to your home directory. Remember to replace `~/ [path name]` with `$HOME`, if necessary.

How to Navigate Through the Linux Filesystem

Procedure Reference: Change Directories

To change directories:

1. Log in as a user in the CLI.
2. To view the present working directory, enter `pwd`.
3. To change to the target directory, enter `cd {absolute or relative path of the target directory}`.
4. If necessary, to verify if you have changed to the target directory, enter `pwd`.

Procedure Reference: List Files and Directories

To list files and directories:

1. Log in as a user in the CLI.
2. To list the files and directories, enter the `ls [options]` command.

Procedure Reference: Work with Files and Directories Using the Nautilus Browser in Spatial Mode

To work with files and directories using the Nautilus browser in spatial mode:

1. Log in as a user in the GUI.
2. Double-click the **Computer** icon on the desktop.
3. Double-click the desired directory to open it.
4. Double-click the desired file in the directory.
5. If necessary, to close all parent windows, press **Ctrl+Shift+W**.
6. To close the Nautilus browser, click the **Close** button.

Procedure Reference: Work with Files Using the Nautilus Browser in Browser Mode

To work with files using the Nautilus browser in browser mode:

1. Log in as a user in the GUI.
2. From the menu bar, choose **Application→System Tools→File Browser**.
3. Double-click the desired file or directory either in the right pane or in the left pane to view it.
4. Close the Nautilus browser.

Procedure Reference: Set the Nautilus Browser to Open Always in Browser Mode

To set the Nautilus browser to open always in browser mode:

1. Log in as user in the GUI.
2. Double-click the **Computer** icon on the desktop.
3. In the Computer window, choose **Edit→Preferences**.
4. In the **File Management Preferences** dialog box, select the **Behavior** tab.

- 5. In the **Behavior** section, check the **Always open in browser windows** check box and click **Close**.
- 6. Close the Computer window.
- 7. To open the Nautilus browser in browser mode, double-click the **Computer** icon.

ACTIVITY 3-2

Changing Directories

Before You Begin:

You have logged in as root in the CLI.

Scenario:

You have been hired as a junior administrator in an organization and provided administrative access to your Linux system. However, as the superuser, you do not have a specified directory in /home to work in. You therefore decide to switch to the home directory and work with files.

What You Do	How You Do It
1. Switch from the /root directory to the /home directory.	<div>a. To view the current working directory, enter <code>pwd</code></div> <div>b. Observe that the current working directory is /root. To change to the home directory, enter <code>cd /home</code></div> <div>c. To view the current working directory, enter <code>pwd</code></div> <div>d. Observe that the current working directory is now changed to /home.</div>
2. List the files in the directory.	<div>a. To list all the files in the /home directory, enter <code>ls -a</code></div> <div>b. Observe the listed files in the directory. To clear the terminal screen, enter <code>clear</code></div>

ACTIVITY 3-3

Using the Nautilus Browser to View File and Directory Content

Before You Begin:

1. You have logged in as root in the first terminal.
2. Switch to the GUI.
3. Log in as root.

Scenario:

A new employee needs assistance on basic filesystem navigation and usage in the GUI. You decide to demonstrate the usage of the Nautilus browser by navigating through file content.

What You Do	How You Do It
1. Open directories using the Nautilus browser in spatial mode.	<ol style="list-style-type: none">a. Double-click the Computer icon on the desktop.b. In the Computer window, double-click the Filesystem object.c. Observe that the content opens in a different window, and view the contents of the directory. Close the / directory window.

2. Set the Nautilus browser to open in browser mode and view directory content.
 - a. In the Computer window, choose **Edit**→**Preferences**.
 - b. To change the behavior of the browser window, in the **File Management Preferences** dialog box, select the **Behavior** tab.
 - c. To enable the windows to open in browser mode, in the **Behavior** section, check the **Always open in browser windows** check box and click **Close**.
 - d. Close the Computer window.
 - e. To verify the changes made, double-click the **Computer** icon on the desktop.
 - f. Observe that the Nautilus browser opens in browser mode. To view the contents of the **/** directory, in the left pane, double-click the **File System** object.
 - g. Observe the contents of the directory.
 - h. Close the browser window.
-
-

TOPIC C

Manage the Filesystem

Now that you can navigate through the Linux filesystem, it is time to learn how to manage it. In this topic, you will manage the Linux filesystem.

Managing the Linux filesystem will allow you to customize the system to suit your requirements. Also, you will be able to organize files and directories, mount additional drives, and use recordable media for backups or storage.

Filesystem Management Tasks

While managing a filesystem in Linux, you will perform the following tasks:

- Back up files and directories.
- Mount and unmount filesystems.
- And, create swap space on a disk partition.

Burning Discs

While managing your filesystem, you may have to back up some data in discs. Linux allows you to burn CDs and DVDs with GUI-based programs, as well as from the CLI. GUI-based programs guide you through the burning process. To burn a disc from the CLI:

1. Create a directory and copy the files you would like to burn.
2. Make an ISO image of the files using the `mkisofs` command.
3. And, burn the CD using the `cdrecord` command.

 You must have a CD or DVD writer installed on your system to be able to burn discs.


ISO Images

An *ISO image* or *disk image* is an archive file format for files that are to be written to optical discs such as CDs and DVDs. It is a standard defined by the International Organization for Standardization (ISO) and has a file extension of `.iso`.

Mount Points

Definition:

A *mount point* is an access point to information stored on a local or remote storage device. The mount point is typically an empty directory on which a filesystem is loaded, or mounted, to make the filesystem accessible to users. If the directory already has content, the content becomes invisible to the users until the mounted filesystem is unmounted.

 You can use the `/etc/fstab` file to list the filesystem to be mounted and unmounted when the Linux system boots and shuts down, respectively.

Example:

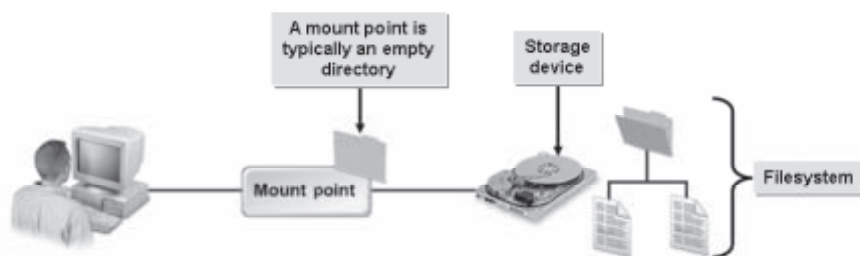


Figure 3-15: The process of mounting a filesystem.

The mount Command

In Linux, a filesystem cannot be accessed directly. It has to be associated with a directory to make it accessible to users. This association is brought about by loading, or mounting, the filesystem in a directory by using the `mount` command. After using the filesystem, it needs to be disassociated from the directory by unloading, or unmounting, the filesystem using the `umount` command.

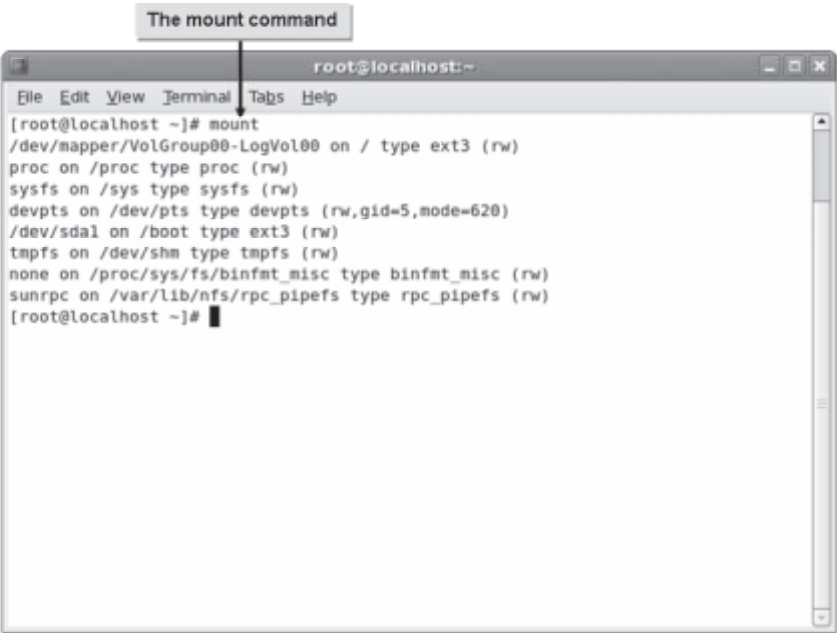


Figure 3-16: A list of currently mounted filesystems.

mount Command Options

You can specify various mount options for a filesystem.

Option	Enables You To
auto	Specify that the device has to be mounted automatically.
noauto	Specify that the device need not be mounted automatically.
nouser	Specify that only the root user can mount a device or a filesystem.
user	Specify that all users can mount a device or a filesystem.
exec	Allow binaries in a filesystem to be executed.
noexec	Prevent binaries in a filesystem from being executed.
ro	Mount a filesystem as read-only.
rw	Mount a filesystem with read and write permissions.
sync	Specify that input and output operations in a filesystem should be done synchronously.
async	Specify that input and output operations in a filesystem should be done asynchronously.

Binaries

Binaries are source codes that are compiled into executable programs, or are assembled so that they are readable by the computer system. Binaries are encoded so that they can be transmitted over the Internet. In addition, binaries can be pictures, word processing files, or spreadsheet files. Some binaries may contain viruses that can harm the system.

Swap Space

Definition:

Swap space is a partition on the hard disk that is used when the system runs out of physical memory. Linux pushes some of the unused files from the RAM to the swap space to free up memory. Usually, the swap space equals twice the RAM capacity.

Example:

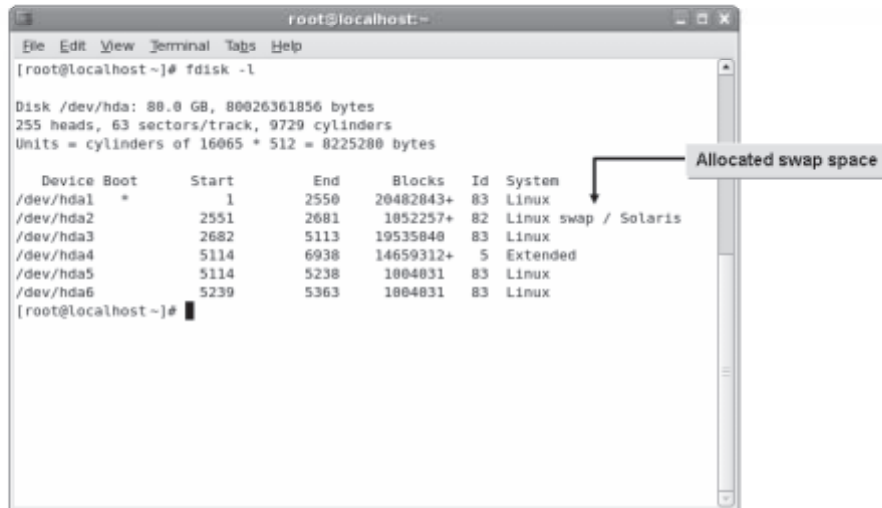


Figure 3-17: Swap space being created on a hard disk.

Swap space can be one of three types.

Swap Type	Description
Device swap	Device swap space is configured when you partition the hard disk. It is used by the operating system to run large applications.
Filesystem swap	Filesystem swap space is configured primarily when you install Linux. It is utilized by the operating system as an emergency resource when the available swap space runs out.
Pseudo-swap	Pseudo-swap space allows large applications to run on computers with limited RAM.

Swap Files

Swap files are created for storing data that is to be transferred from a system's memory to a disk. It is dynamic and changes in size when data is moved in and out of the memory. It is used as a medium to transfer data from the RAM on to the hard disk.

Swap Partitions

A swap partition is an area of virtual memory on a hard disk to complement the physical RAM in the computer. Swap partitions are created by Linux because they perform better than swap filesystems.

The mkswap Command

mkswap is a system administration command that is used to create swap space on a disk partition. It provides options to perform various tasks.

Option	Enables You To
-c	Verify that the device is free from bad sectors before mounting the swap space.
-f	Force a swap partition of an area larger than the permissible limit.
-p	Set the page size to be used by the <i>mkswap</i> command.
-L {label}	Activate the swap space using labels applied to partitions or filesystems.

Syntax

The syntax of the *mkswap* command is *mkswap [options] device {size}*. The device argument of *mkswap* is generally a disk partition, such as */dev/hda2* or */dev/sdb3*, but it can also be a file.

Swap Partition Management Commands

A number of commands are used to manage swap partitions. The most important commands are *swapon* and *swapoff*.

Command	Description
<i>swapon</i>	Used to activate a swap partition on a specified device. It provides a number of options for specifying devices.
<i>swapoff</i>	Used to deactivate the swap space on devices.

The swapon and swapoff Command Options

Some of the frequently used *swapon* and *swapoff* command options are given in the following table.

Option	Description
<i>swapon -e</i>	It is used to skip devices that do not exist.
<i>swapon -a</i>	It is used to activate all the swap space.
<i>swapoff -a</i>	It is used to deactivate all the swap space.

How to Manage the Linux Filesystem

Procedure Reference: Create a Mount Point

To create a mount point:

1. Log in as root.
2. To create a mount point, enter `mkdir {mount point}`.
3. To set the user as the owner of the mount point, enter `chown {user name} {mount point}`.
4. To set the group as the owner of the mount point, enter `chgrp {group name} {mount point}`.

The chgrp Command

The `chgrp` command is used to change the group ownership of one or more files or directories.

Procedure Reference: Mount a Filesystem

To mount a filesystem:

1. Log in as root in the CLI.
2. To mount the specified device on the specified mount point, enter `mount [options] /dev/{device name}{partition number} {mount point}`.
3. To verify that the filesystem is mounted on the specified mount point, enter `mount {mount point}`.

Procedure Reference: Mount Filesystems at Startup

To mount filesystems at startup:

1. Log in as root in the CLI.
2. To open the `/etc/fstab` file, enter `vi /etc/fstab`.
3. To add an entry for the new filesystem, type `{filesystem label} {device or partition name} {mount point} {filesystem type} {mount options} {dump options} {fsck options}`.
4. Save and close the file.
5. To reload the mount table with recent changes from the `/etc/fstab` file, reboot the system or enter `mount -a`.
6. Verify that the filesystem has been automatically mounted at startup.
 - a. Log in as root.
 - b. To view all the mounted filesystems, enter `mount`.

Procedure Reference: Unmount a Filesystem

To unmount a filesystem:

1. Log in as root in the CLI.
2. Unmount a filesystem.

- To unmount the filesystem, enter `umount [options] /dev/{device name}{Partition number}`.
- Or, enter `umount [options] {mount point}`.

Procedure Reference: Manage a Filesystem

To manage a filesystem:

1. Log in as root in the CLI.
2. To display the details about the processes using the filesystem, enter `fuser {mount point}`.
3. To kill all processes using the filesystem, enter `fuser -km {mount point}`.
4. To unmount the filesystem, enter `umount {mount point}`.



The filesystem cannot be unmounted while it is being used by another process.

Procedure Reference: Manage Swap Partitions

To manage swap partitions:

1. Log in as root in the CLI.
2. To create a swap partition, enter `mkswap /dev/{device name}{partition number}`.
3. To add the partition entry, open the `/etc/fstab` file in `vi` and type `{filesystem label}{device name}{partition number} none swap {mount options} {dump options} {fsck options}`.
4. To activate the swap partition, enter `swapon {device name}`.
5. To deactivate the swap partition and convert it into a standard Linux filesystem, enter `swapoff {device name}`.

Procedure Reference: Format a Partition with a Filesystem

To format a partition with a filesystem:

1. Log in as root in the CLI.
2. Format a partition with a filesystem.
 - To create a specified filesystem on a specified partition of the device, enter `mkfs -t {filesystem type} /dev/{device name}{partition number}`.
 - Or, to create an ext2 filesystem on the specified partition of the device, enter `mke2fs [options] /dev/{device name}{partition number}`.

ACTIVITY 3-4

Mounting Filesystems

Before You Begin:

1. You have logged in as root in the GUI.
2. Switch to the CLI.
3. To create the user netadmin2, at the command line, enter `useradd netadmin2`.
4. To set the password for netadmin2, enter `passwd netadmin2`.
5. To set the password for netadmin2, at the **New UNIX password** prompt, enter `myp$$w0rd`.
6. Confirm the password by retyping the same password at the prompt.
7. To unmount the /dev/sdb5 partition, enter `umount /dev/sdb5`.
8. To unmount the /dev/sdb6 partition, enter `umount /dev/sdb6`.
9. To change to the root directory, enter `cd /root`.
10. To clear the terminal screen, enter `clear`.

Scenario:

There is a meeting at your office. A couple of users want to have their systems moved to the conference room so that they can access their files during the conference. You find that there are multiple systems to be moved, and this will take a lot of time. Therefore, you decide to take the required files from the users and load them on the system in the conference room in separate partitions, so that the users can access their files.


Use the following user and partition details to mount the filesystems:

- User name: netadmin1, Partition size: 1 GB, Mount point: /admin1, User and group owner of /admin1: netadmin1
- User name: netadmin2, Partition size: 1 GB, Mount point: /admin2, User and group owner of /admin2: netadmin2

LESSON 3

What You Do	How You Do It
1. Create mount points for users.	<ol style="list-style-type: none">Enter mkdir /admin1To set the netadmin1 user as the owner of /admin1 mount point, enter chown netadmin1 /admin1To set the netadmin1 group as the owner of /admin1 mount point, enter chgrp netadmin1 /admin1Create a mount point, /admin2, and assign user ownership and group ownership to netadmin2 by following the steps from (a) to (c).To clear the terminal screen, enter clear
2. Mount and verify the filesystem.	<ol style="list-style-type: none">To mount the filesystem for netadmin1, enter mount -a /dev/sdb5 /admin1To view the mounted partitions, enter mountObserve that the line “/dev/sdb5 on /admin1 type ext2 (rw)” is displayed, indicating that the filesystem is mounted.To mount the filesystem for netadmin2, enter mount -a /dev/sdb6 /admin2To view the mounted partitions, enter mountObserve that the line “/dev/sdb6 on /admin2 type ext2 (rw)” is displayed, indicating that the filesystem is mounted.

3. Create an entry in the `fstab` file to mount the `/dev/sdb5` and `/dev/sdb6` filesystems when the system boots.
 - a. To open the `fstab` file, enter **vi /etc/fstab**
 - b. To go to the last line, press **Shift+G**.
 - c. To switch a new line in insert mode, press **O**.

 Insert mode allows you to insert text by typing.
 - d. To mount the `/dev/sdb5` filesystem when the system boots, enter **/dev/sdb5 /admin1 ext2 defaults 0 0**
 - e. To mount the `/dev/sdb6` filesystem when the system boots, type **/dev/sdb6 /admin2 ext2 defaults 0 0**
 - f. Press **Esc**.
 - g. Save and close the file.
 - h. To clear the terminal screen, enter **clear**
 - i. To update the `fstab` file, enter **mount -a**

 4. Check that the specified filesystem mounts when the system boots.
 - a. To reboot the system, enter **reboot**
 - b. To switch to the CLI, press **Ctrl+Alt+F1**.
 - c. Log in as **root** in the CLI of the Linux system.
 - d. To verify that the filesystems are mounted at the specified mount points on boot, enter **mount**
 - e. Observe that the partitions `/dev/sdb5` and `/dev/sdb6` are mounted into the `/admin1` and `/admin2` directories, respectively.
 - f. To clear the terminal screen, enter **clear**
-

TOPIC D

Maintain the Filesystem

After managing a Linux filesystem, it is important to learn how to keep it up and running. In this topic, you will maintain the Linux filesystem.

Maintaining the Linux filesystem will assist you in troubleshooting and general maintenance of your system. If a power outage or other unplanned shutdown occurs, you will need to know how to verify the data integrity of your local drives.

Filesystem Maintenance Tasks

Maintaining a filesystem in Linux involves the following tasks:

- Checking the integrity of the filesystem.
- Managing the size of partitions.
- Removing temporary files.
- And, performing system recovery.

Storage Devices

There are different types of storage devices in Linux. Each device has a particular use associated with it.

Device	Description
Hard disk	An internal device that can store large amounts of data. It can be accessed quickly.
Floppy drive	A removable medium that can store smaller amounts of data. It cannot be accessed as quickly as a hard disk.
Tape drive	A device that is used to store large amounts of data on a magnetic tape. Tape drives can be internal or external. External tape drives are portable, whereas in internal tape drives only the tape is removable. Data is accessed sequentially in a tape drive.
Zip drive	A portable storage device that precedes the flash drive.
Flash drive	A small, portable, storage device that is used to store files that need to be carried around.
CD-R(W)	A removable optical disc that stores 650-700 MB of data. It can be accessed faster than other removable storage media.
DVD-R(W)	A removable optical disc that stores 4.5 GB (or more) of data. It can be accessed faster than other removable storage media.

Mass Storage Devices

Mass storage devices are types of storage devices that provide fast access to large amounts of data in a small, reasonably reliable, physical package. Hard disks, tape drives, flash drives, CD-R(W), DVD-R(W), and zip drives are some of the common mass storage devices.

ATAPI

AT Attachment Packet Interface (ATAPI) is a protocol for controlling mass storage devices. ATAPI provides commands that are used for hard disks, CD-ROM drives, tape drives, and other devices.

Journaling Filesystems

A *journaling filesystem* is a method that is used by an operating system to quickly recover after an unexpected interruption, such as a system crash. Journaling filesystems can remove the need for a filesystem check when the system boots. By using journaling filesystems, the system does not write modified files directly on the disk. Instead, a journal is maintained on the disk. The journaling filesystem process involves the following phases:

1. The journal describes all the changes that must be made to the disk.
2. A background process makes each change as and when it is entered in the journal.
3. If the system shuts down, pending changes are performed when it is rebooted.
4. And, incomplete entries in the journal are discarded.

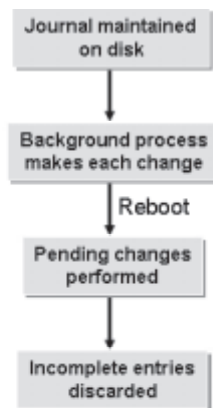


Figure 3-18: Stages in the journaling process.

Performance Issues with Journaling

A journaled filesystem works well with small files and small drives. With the growth of file and drive sizes, performance will suffer. Some of the reasons for poor performance include:

- Filesystem recovery time after a power failure or improper shutdown.
- Bitmap method of tracking the filesystem.
- Wasted space and fragmentation.

The fsck Command

The *fsck* command is used to check the integrity of a filesystem. *Filesystem integrity* refers to the correctness and validity of a filesystem. Most systems automatically run the *fsck* command at boot time so that errors, if any, are detected and corrected before the system is used. Filesystem errors are usually caused by power failures, hardware failures, or improper shutdown of the system.

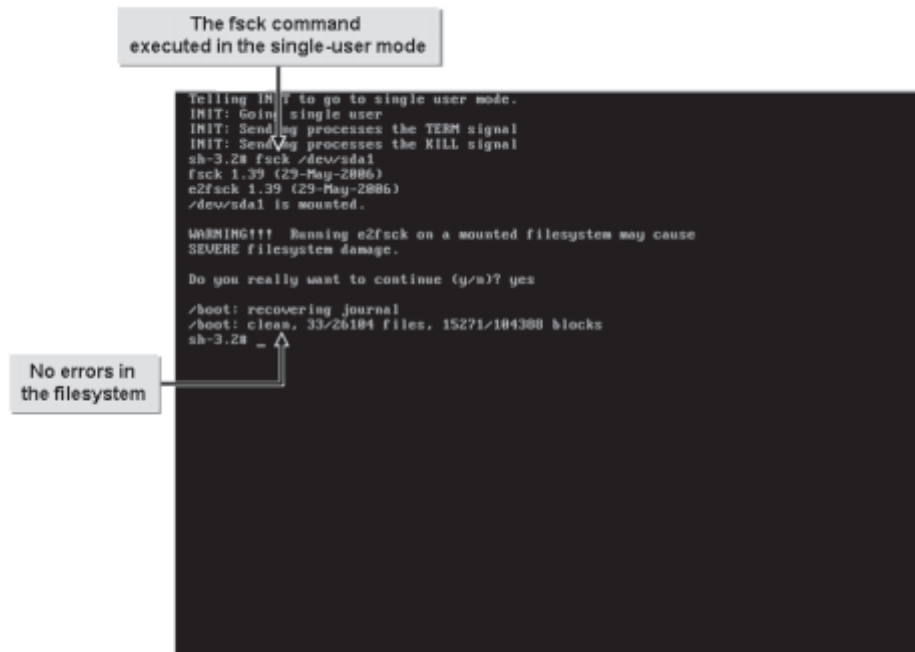


Figure 3-19: Checking the integrity of a filesystem from single-user mode.

Syntax

The syntax of the `fsck` command is `fsck -t {filesystem type} [options]`.

Repair Filesystems

You can use the `fsck -r /dev/{filesystem}` command to repair a filesystem. The command will prompt you to confirm your actions. If you are simultaneously checking multiple filesystems, you should not use this option because it allows you to repair only a single filesystem at a time.

The e2fsck Command

The `e2fsck` command allows you to check the ext2, ext3, and ext4 filesystems. You need to unmount the filesystem before running the `e2fsck` command to prevent damage to the filesystem.

The syntax of the `e2fsck` command is `e2fsck /dev/{filesystem}`.

The tune2fs Utility

The `tune2fs` utility helps tuning parameters associated with a Linux filesystem. Using this utility, a journal can be added to an existing ext2 or ext3 filesystem. If the filesystem is already mounted, the journal will be visible in the root directory of the filesystem. If the filesystem is not mounted, the journal will be hidden. The `tune2fs` utility is available with most Linux distributions.

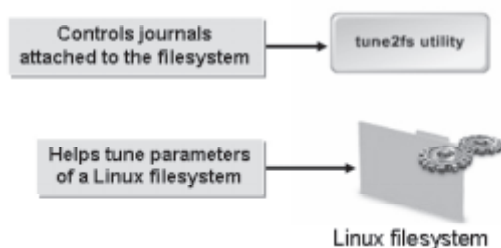


Figure 3-20: The *tune2fs* utility is used to manage filesystems.

Tunable Parameters

Using the *tune2fs* utility, you can adjust the parameters of the extended filesystems, such as ext2, ext3, and ext4, that can be tuned on a Linux machine even after installation. Tunable parameters allow you to remove reserved blocks; alter reserved block count; and specify the number of mounts between checks, the time interval between checks, and the behavior of the kernel code, among others.

Options of the *tune2fs* Utility

The *tune2fs* utility has various options.

Use This Option	To Do This
<code>-j {partition}</code>	Convert the existing filesystem to an ext3 filesystem.
<code>-i d m w</code>	Specify the maximum time interval between filesystem checks in days, months, or weeks.
<code>-c maximum mounts count</code>	Specify the maximum number of mounts between filesystem checks.
<code>-C mount count</code>	Specify the number of times the filesystem can be mounted.
<code>-r reserved blocks count</code>	Specify the number of reserved filesystem blocks.
<code>-e continue remount-ro panic</code>	Specify the behavior of the kernel code, whether the filesystem should continue with normal execution, remount the filesystem in read-only mode, or cause a kernel panic, when errors are detected.
<code>-l</code>	List the contents within the superblock of the filesystem.
<code>-U UUID</code>	Set the specified Universally Unique Identifier (UUID) for the filesystem.

Syntax

The syntax of the *tune2fs* utility is *tune2fs [options] {device name}*.

The *dumpe2fs* Utility

The *dumpe2fs* utility is used for managing ext2, ext3, and ext4 (extended) filesystems. It dumps the status of the extended filesystem onto the standard output device and prints the block group information for the selected device.

LESSON 3

The `dumpe2fs` utility has various options.

Option	Enables You To
-x	Print a detailed report about block numbers in the filesystem.
-b	Print the bad blocks in the filesystem.
-f	Force the utility to display the filesystem status irrespective of the filesystem flags.
-i	Display filesystem data from an image file created using the <code>e2image</code> utility.

Syntax

The syntax of the `dumpe2fs` command is `dumpe2fs [options] [block size] {device name}`.

The debugfs Utility

The `debugfs` utility allows you to examine and modify ext2, ext3, and ext4 filesystem. When executed, the `debugfs` utility opens an interactive shell that can be used to examine and modify the extended filesystem.

Commands Supported by the debugfs Utility

The table provides some common commands supported by the `debugfs` utility in the interactive shell.

If You Need To	Use This Command
Open a filesystem	<code>open /dev/{filesystem}</code>
Close the filesystem	<code>close</code>
View the filesystem information	<code>stats</code>
Find a free block	<code>ffb</code>

xfs Tools

There are many xfs tools that allow you to work with the xfs filesystem.

xfs Tool	Enables You To
<code>xfs_info</code>	Display details about the xfs filesystem.
<code>xfs_metadump</code>	Copy the metadata information of the xfs filesystem to a file.
<code>xfs_grow</code>	Expand the xfs filesystem to fill the disk size.
<code>xfs_repair</code>	Repair and recover a corrupt xfs filesystem.
<code>xfs_db</code>	Debug the xfs filesystem.

How to Maintain the Linux Filesystem

Procedure Reference: Create ext2 Filesystems

To create ext2 filesystems:

1. If you already have a mounted drive with an existing filesystem:
 - a. Back up all data on the drive to removable media or another drive.
 - b. Unmount the drive using the `umount` command.
 - c. Build the ext2 filesystem using the `mkfs -t` command.
2. If you have an empty drive:
 - a. Build the ext2 filesystem using the `mkfs -t` command.
3. Mount the drive using the `mount` command.
4. To reflect the changes that were done to the filesystem, update the `/etc/fstab` file.

Procedure Reference: Create ext3 Filesystems

To create ext3 filesystems:

1. If you have a drive with the ext2 filesystem:
 - a. Unmount the drive using the `umount` command.
 - b. Convert the filesystem using the `tune2fs -j {partition}` command.
2. If you already have a mounted drive with an existing filesystem other than ext2:
 - a. Back up all data on the drive to removable media or another drive.
 - b. Unmount the drive using the `umount` command.
 - c. Build the ext3 filesystem using the `mkfs -t` command.
 - d. Mount the drive using the `mount` command.
3. If you have an empty drive:
 - a. Build the ext3 filesystem using the `mkfs -t` command.
 - b. Mount the drive using the `mount` command.
4. To reflect the changes that were done to the filesystem, update the `/etc/fstab` file.

Procedure Reference: Create reiserfs Filesystems

To create reiserfs filesystems:

1. Verify that you have a kernel version later than 2.4.16.
2. If you already have a mounted drive with an existing filesystem:
 - a. Back up all data on the drive to removable media or another drive.
 - b. Unmount the drive using the `umount` command.
 - c. Build the reiserfs filesystem using the `mkreiserfs` command.
 - d. Mount the drive using the `mount` command.
 - e. To reflect the changes that were done to the filesystem, update the `/etc/fstab` file.
3. If you have an empty drive:
 - a. Build the reiserfs filesystem using the `mkfs -t reiserfs` command.

- b. Mount the drive using the `mount` command.
- c. Add the drive to the `/etc/fstab` file.

Procedure Reference: Manage Local Filesystems

To manage local filesystems:

1. Switch to single-user mode.
2. Check the filesystem using the `fsck` command.
3. Return to multiuser mode after the check is complete.

Procedure Reference: Manage the ext2 Filesystem Using the debugfs Utility

To manage an ext2 filesystem using the `debugfs` utility:

1. Log in as root in the CLI.
2. To access the `debugfs` prompt, enter `debugfs /dev/{filesystem}`.
3. To view the commands that are supported in this prompt, at the `debugfs` prompt, enter `help`.
4. Enter *{command supported by debugfs}*.
5. To quit the `debugfs` command prompt, enter `quit`.

ACTIVITY 3-5

Maintaining the Linux Filesystem

Before You Begin:

1. You have logged in as root in the CLI.
2. To switch to runlevel 3, enter `telinit 3`.
3. To continue in the new runlevel, press **Enter**.
4. To clear the terminal screen, enter `clear`.

Scenario:

Due to a thunderstorm, there was a brief power outage overnight and the Linux systems were not shutdown properly. The systems need to be checked for consistency. Using the `fsck` command, verify the drive and data integrity of the hard disk.

What You Do	How You Do It
1. Run the <code>fsck</code> command on the local filesystem.	<ul style="list-style-type: none">a. To switch to single-user mode, enter <code>telinit 1</code>b. Enter <code>fsck /dev/sdb1</code>c. At the warning prompt, press Y.d. Observe that the message displays "clean", which indicates that there is no error in the filesystem.e. To switch to runlevel 3, enter <code>telinit 3</code>
2. At which runlevel can you perform disk maintenance without damaging the disks? <ul style="list-style-type: none">a) Runlevel 0b) Runlevel 1c) Runlevel 3d) Runlevel 5	
3. True or False? You can run the <code>e2fsck</code> command to perform a disk check on a mounted filesystem. <ul style="list-style-type: none">___ True___ False	

ACTIVITY 3-6

Configuring the ext3 Filesystem

Before You Begin:

- 1. The Linux system is running in runlevel 3.
- 2. Log in as root.
- 3. To switch to the GUI, enter `telinit 5`.
- 4. Switch to the first CLI terminal.
- 5. To continue, press **Enter**.
- 6. To clear the terminal screen, enter `clear`.

Scenario:

Two users complain that they lost data due to improper shutdown of the system. You run the disk check utility and verify that the disk is not corrupt. Further, you decide to convert the existing filesystem to a journaling filesystem to ensure that data will not be lost even if the system is accidentally turned off.

What You Do	How You Do It
1. Unmount the /dev/sdb5 and /dev/sdb6 partitions.	<ul style="list-style-type: none">a. To view the mounted partitions, enter mountb. Observe that the two partitions, /dev/sdb5 and /dev/sdb6, are mounted automatically. To unmount the /dev/sdb5 partition, enter umount /dev/sdb5c. To unmount the /dev/sdb6 partition, enter umount /dev/sdb6d. To view the mounted partitions, enter mounte. Observe that the two partitions, /dev/sdb5 and /dev/sdb6, are not listed indicating that they have been unmounted.

2. Convert the /dev/sdb5 and /dev/sdb6 partitions to the ext3 filesystem.
 - a. To convert the partition to the ext3 filesystem, enter **tune2fs -j /dev/sdb5**
 - b. Observe the details displayed during the conversion of the filesystem. To convert the partition to the ext3 filesystem, enter **tune2fs -j /dev/sdb6**
 - c. Observe the details displayed during the conversion of the filesystem. To clear the terminal screen, enter **clear**

3. Verify that the two new partitions have the ext3 filesystem.
 - a. To start the **GNU Parted** utility, enter **parted**
 - b. To select the /dev/sdb partition, enter **select /dev/sdb**
 - c. To view the list of existing partitions, at the **(parted)** prompt, enter **print**
 - d. Observe that the partitions 5 and 6 have the **ext3** filesystem. To quit from the **parted** utility, enter **q**
 - e. To clear the terminal screen, enter **clear**

LESSON 3

4. Modify the partition entries in the fstab file to mount the ext3 filesystems when the system boots.
 - a. To open the fstab file, enter **vi /etc/fstab**
 - b. Navigate to the line containing the **"/dev/sdb5"** entry and place the cursor on the number 2 in **"ext2."**
 - c. To switch to insert mode, press **I**.
 - d. Type **3** and press **Delete**.
 - e. To navigate to the line containing the **"/dev/sdb6"** entry, press the **Down Arrow** key and the **Left Arrow** key and place the cursor after the number 2 in **"ext2."**
 - f. Type **3** and press **Delete**.
 - g. Press **Esc**.
 - h. Save and close the file.
 - i. To clear the terminal screen, enter **clear**
 - j. To update fstab entries, enter **mount -a**
 - k. To reboot the system, enter **reboot**

 5. Check that the specified filesystem mounts when the system boots.
 - a. To switch to the CLI, press **Ctrl+Alt+F1**.
 - b. Log in as **root** in the CLI of the Linux system.
 - c. To view the mounted partitions, enter **mount**
 - d. Observe that the two partitions, **/dev/sdb5** and **/dev/sdb6**, have **"ext3"** as the filesystem.
 - e. To clear the terminal screen, enter **clear**
-
-

Lesson 3 Follow-up

In this lesson, you created partitions and filesystems on the hard disk. Knowledge of the filesystem structure assists you in navigating, managing, and maintaining filesystems efficiently.

1. **When do you think formatting a partition is necessary? Why?**

2. **Is the ext3 filesystem better than the ext2 filesystem? How?**

LESSON 4

Managing Files in Linux

Lesson Time

2 hour(s), 15 minutes

In this lesson, you will manage various files in Linux.

You will:

- Create a text file in Linux.
- Locate files within the Linux filesystem.
- Search text files using regular expressions.
- Apply filters to text streams.
- Manage links to a file.
- Back up and restore files.
- Manage a database using MySQL.

Introduction

In the previous lesson, you managed the Linux filesystem. Now, it is time to learn how to manipulate files and directories within Linux. In this lesson, you will manage various types of Linux files.

As a Linux administrator, you should keep your files well organized on your system. Learning how to create, edit, locate, link, back up, and restore files will help you tailor the system to your needs.

This lesson covers all or part of the following CompTIA Linux+ Powered by LPI certification objectives:

- Topic A:
 - Objective 103.8
- Topic B:
 - Objective 103.3, Objective 103.7, Objective 104.7, Objective 110.1
- Topic C:
 - Objective 103.7
- Topic D:
 - Objective 103.2, Objective 103.7
- Topic E:
 - Objective 104.6
- Topic F:
 - Objective 103.3
- Topic G:
 - Objective 105.3

TOPIC A

Create and Edit Files

In the last lesson, you worked with several Linux filesystem types. Now, you can move on to creating and editing files within those filesystems. In this topic, you will create and edit files.

Working with text files is a basic and routine task for most users. Consider a scenario where you may need to submit a report on your current project. You will require an application, such as a text editor, to create the report. You can also use a text editor to create and edit configuration files, which will allow you to customize your system.

Text Editors

Definition:

A *text editor* is an application that allows you to view, create, or modify the contents of text files. It was originally created to write programs, but is now being used even to edit ordinary text files. Text editors work on different modes such as command mode and insert mode. Various types of text editors, such as Vim, gedit, and nano, are compatible with Linux. However, text editors do not always support the formatting options that word processors provide. Text editors may work either in the CLI or GUI.

Example:

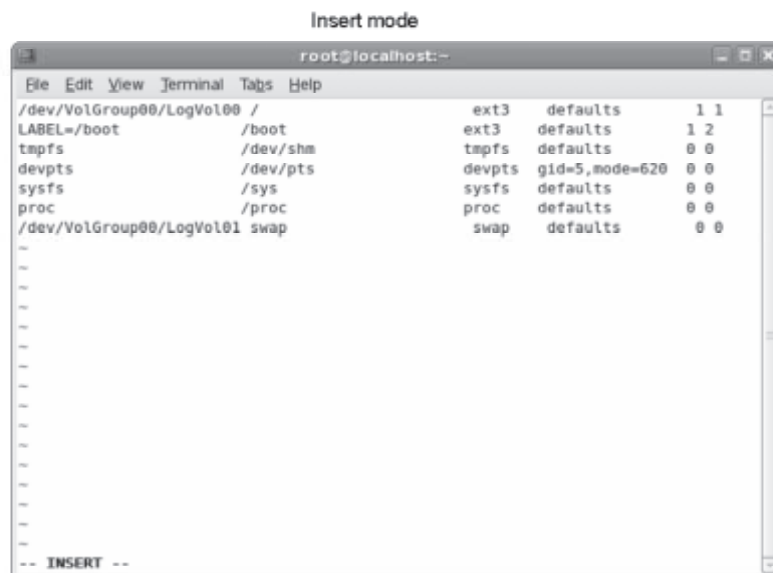


Figure 4-1: The Vim text editor in insert mode.

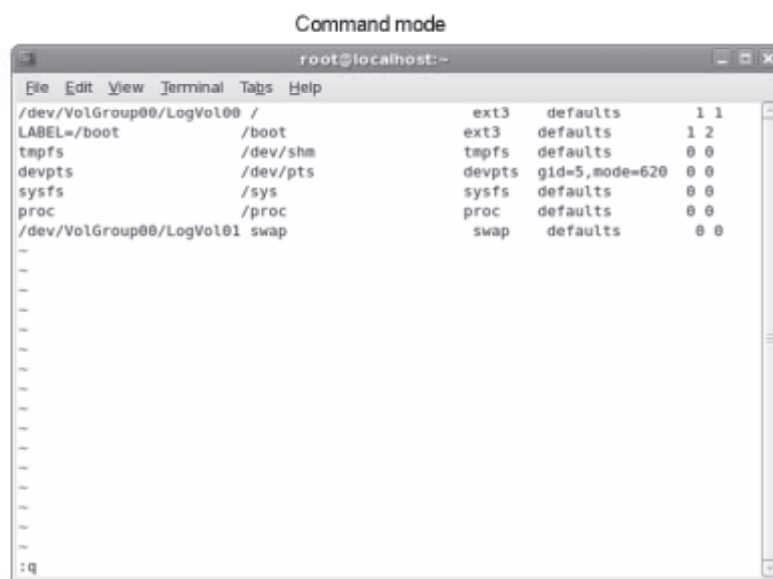


Figure 4-2: The Vim text editor in command mode.

List of Text Editors

Many text editors are compatible with Linux.

Text Editor	Description
<i>Vim</i>	The <i>Vi</i> Improved, or VIM, text editor is the default text editor in Linux. It is widely used in programming and for processing simple text files. It is a powerful editor that optimizes speed by employing simple keystrokes to perform complex text editing.
<i>Emacs</i>	A flexible, powerful, and popular text editor used in Linux and Unix. It offers numerous features such as content-sensitive editing modes and support for various languages. It can be easily customized.
<i>Gvim</i>	The graphical version of the Vim editor.
<i>KWrite</i>	A flexible GUI-based text editor used in KDE.
<i>gedit</i>	A simple yet powerful GUI-based text editor used in the GNOME desktop.
<i>nano</i>	A small, user-friendly text editor that evolved from the Pico text editor.

Emacs

Emacs is derived from “Editor MACroS.” It was written by Richard Stallman.

KDE

KDE is an alternative GUI desktop for Linux. It provides basic desktop functions, applications, tools, and documentation for developers to write applications for the system.

The vim Command

The `vim` command invokes the Vim editor. However, the `vi` command may also be used for this purpose because it automatically redirects the user to Vim. When entered without a file name as an argument, the `vim` command opens a welcome screen by default. To open a file, the syntax `vim {file name}` is used. If the file does not exist, Vim creates a file by the name specified and opens the file for editing. Vim supports multiple files being opened simultaneously.

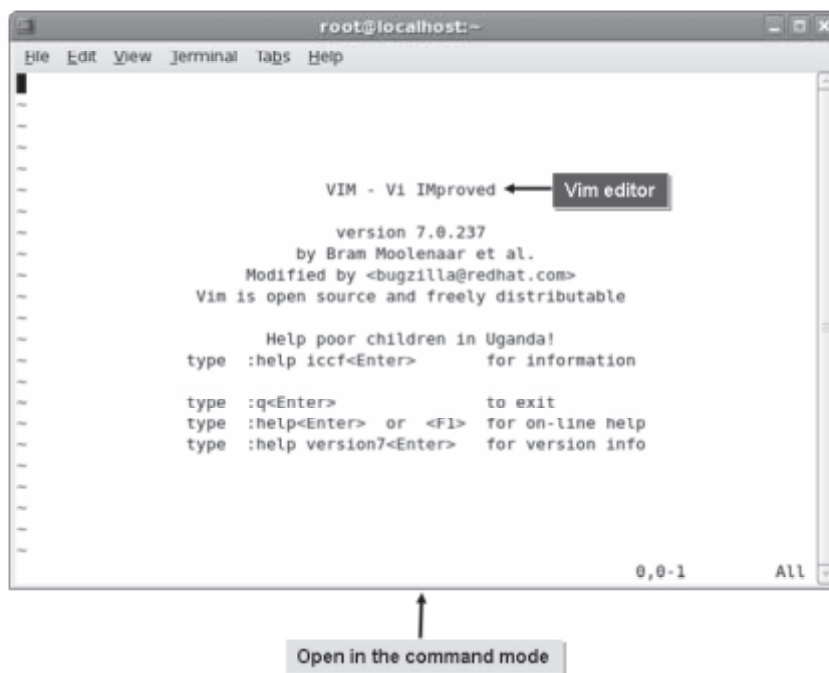


Figure 4-3: The introductory screen of Vim.

Vim Modes

Vim is a modal editor and its different modes decide the functionality of various keys.

Some of the common modes in Vim are listed here.

Mode	Description
<i>Insert</i>	Allows users to insert text by typing.
<i>Execute</i>	Allows users to execute commands within the editor.
<i>Command</i>	Allows users to perform different editing actions using single key-strokes.
<i>Visual</i>	Allows users to highlight or select text for copying, deleting, and so on.

Switch Modes

You can switch between the different modes of Vim. Command mode is the default mode of Vim. You can switch from command mode to any other mode by using a single keystroke.

Some of the keys to switch modes are listed here.

Key	Function
i	Switches to insert mode and inserts text to the left of the cursor.
A	Switches to insert mode and adds text at the end of a line.

Key	Function
I	Switches to insert mode and inserts text at the beginning of a line.
o	Switches to insert mode and inserts text on a new line below the cursor.
O	Switches to insert mode and inserts text on a new line above the cursor.
v	Switches to visual mode to enable selection, one character at a time.
V	Switches to visual mode to enable selection, one line at a time.
:	Switches to execute mode to enable users to enter commands.
Esc	Returns to command mode.

Execute Mode Commands

In command mode, when the colon (**:**) operator is entered, a small command prompt section appears at the bottom-left of the editor. This indicates that the user is in execute mode and can run commands supported by Vim.

Some commands supported by Vim are listed below.

Command	Function
:w {file name}	Saves a file with a file name if it is being saved for the first time.
:q	Quits when no changes have been made after the last save.
:q!	Quits ignoring the changes made.
:qa	Quits multiple files.
:wq	Saves the current file and exits.
:e!	Reverts to the last saved format without closing the file.
:!{any Linux command}	Executes the command and gets the result in the Vim interface.
ZZ	Writes the file only if changes were made and quits the Vim editor.

Vim Help Options

A major source of built-in documentation for Vim can be accessed using the **:help** command. To find topic-specific help, you can add the necessary topic as an argument. To quit the help manual, you can use **:q**. The **vimtutor** command helps first time users learn the basics of Vim by allowing them to practice Vim commands and shortcuts.

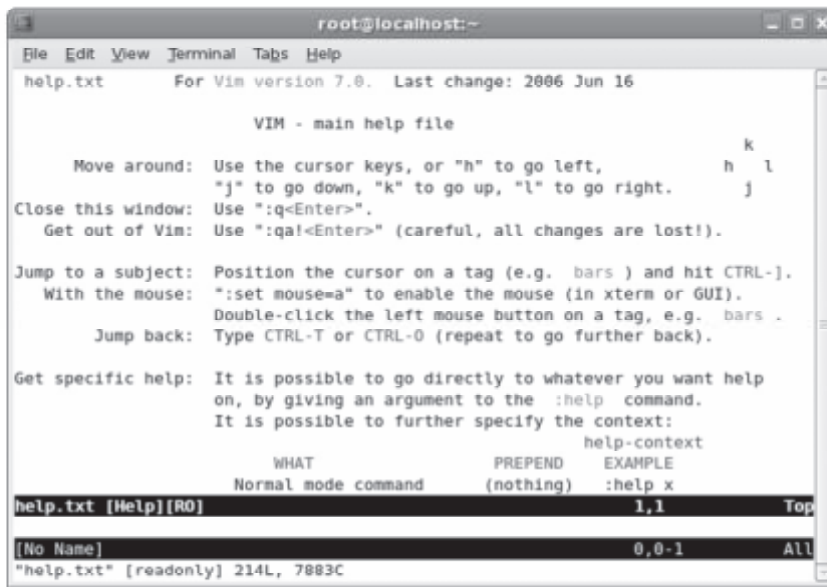


Figure 4-4: Viewing the help file using the Vim text editor.

Motions

Motions are single-key shortcuts that are used to navigate through files in command mode. These keys position the cursor anywhere within a document. They can be used for moving the cursor through characters, words, lines, or even huge blocks of text.

Navigation Key	Used To
H	Move left one character.
J	Move down one line.
K	Move up one line.
L	Move right one character.
^	Move to the beginning of the current line.
\$	Move to the end of the current line.
W	Move to the next word.
B	Move to the previous word.
E	Move to the end of the current word or to the end of the next word if you are already at the end of the word.
Shift+L	Move the cursor to the bottom of the screen.
Shift+H	Move the cursor to the first line of the screen.
(Line number) Shift+G	Move the cursor to the specified line number.
GG	Move the cursor to the first line of the file.
Shift+G	Move the cursor to the last line of the file.

Navigation Using the Arrow Keys


In addition to using the **K**, **J**, **H**, and **L** keys to navigate through the editor, you can also use the **Up**, **Down**, **Left**, and **Right Arrow** keys. The conventional navigation keys such as **Home**, **End**, **Page Up**, and **Page Down** also work in Vim.

Editing Operators

Editing operators in command mode are powerful tools that can be used to manipulate text with simple keystrokes. They can also be used in combination with motions to edit multiple characters.

Some of the frequently used editing operators are listed here.

Editing Operator	Used To
x	Delete the character selected by the cursor.
d	Delete text.
dd	Delete the current line.
p	Paste text on the line directly below the cursor.
P	Paste text on the line directly above the cursor.
/[text string]	Search through the document for specific text.
?[text string]	Search backward through the document for specific text.
y	Yank or copy text.
yy	Copy the line directly above the cursor.
c[range of lines]c	Begin a change in the specified range.
u	Undo the latest change.
U	Undo all changes in the current line.

 In case any editing was undone by mistake, you can press **Ctrl+R** to redo the latest undone changes.

Case Sensitivity

Most Vim options are case sensitive. For example, the **p** option pastes text you cut on the line directly below the cursor, whereas the **P** option pastes text you cut on the line directly above the cursor.

Counts

A *count* is a number that multiplies the effect of keystrokes in Vim. It can be used in combination with motions or operators or both. When used with a motion, cursor movement is multiplied according to the count specified. When used with editing operators, the action gets repeated the number of times specified.

Syntax

If count, motions, and operators are used together, their syntax is `operator [count] {motion}`. This makes the cursor move and perform the action as many times as specified by the count.

The diff Command

The *diff* command is used to compare individual text files or contents of directories. The command displays the two files and the differences between them.

The `diff` command has various options that allow you to specify the nature of the output.

Option	Description
<code>-b</code>	Ignores spacing differences.
<code>-i</code>	Ignores case differences.
<code>-t</code>	Expands tab characters in output lines.
<code>-w</code>	Ignores spacing differences and tabs.
<code>-c</code>	Displays a list of differences with three lines of context. The output displays the identification of the files involved and their creation dates, and each change is separated by a line with a dozen asterisks (*). The lines that are removed from the first file are marked with hyphens (-); those that are added to the second file are marked with the plus sign (+). Lines that are shifted from one file to the other are marked in both the files with exclamation points (!).



Figure 4-5: Comparing two versions of the same document with the *diff* command to track changes.

Syntax

The syntax of the `diff` command is `diff {file name 1} {file name 2}`.

The patch Command

The *patch* command updates text files with changes according to instructions contained in a patch file. This patch file contains listings produced by the `diff` command.

Comparing Text Files

The `vimdiff` command allows you to compare two text files. The syntax of this command is similar to the syntax of the `diff` command.

The wc Command

The *word count* (`wc`) command is used to count the number of lines, words, and characters of text files. If multiple files are specified, then the command displays the count for each file and the total count for all files.

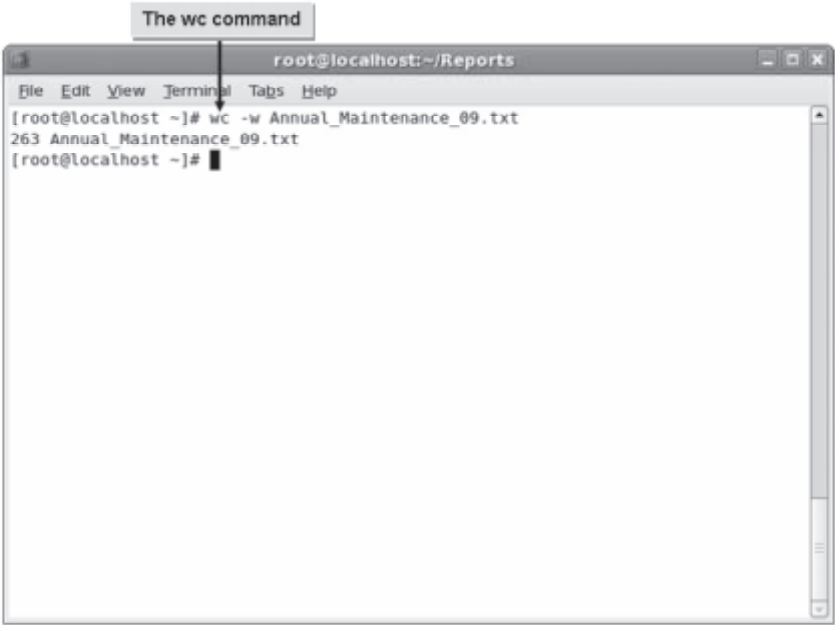


Figure 4-6: Counting words using the `wc` command.

The `wc` command provides various options that allow you to specify the nature of the output.

Option	Description
-c	Displays the byte count.
-m	Displays the character count.
-l	Displays the newline count.
-w	Displays the word count.

Syntax

The syntax of the `wc` command is `wc [options] {file name}`.

The aspell Utility

aspell is a utility that functions as a spell checker in Linux. The syntax of the *aspell* command is *aspell [options]*. The *-c* option checks the file for incorrect spellings. The *-list* option produces a list of misspelled words from the standard input.

The tr Command

The *translate* (*tr*) command is used to translate strings from the standard input to the standard output. It is predominantly used to change the case of letters. This command acts only on a stream of characters and does not accept file names as arguments.

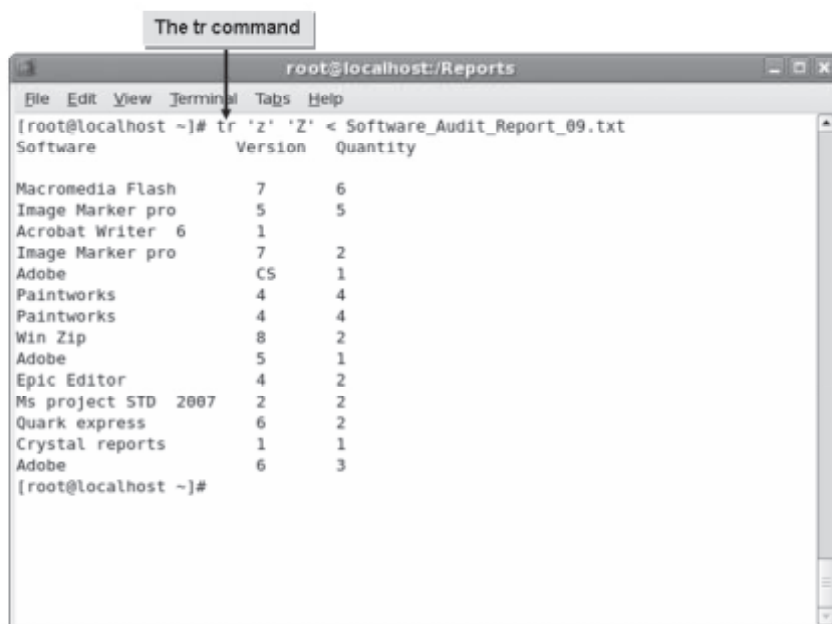


Figure 4-7: Editing text using the *tr* command.

Syntax

The syntax of the *tr* command is *tr {'character 1'} {'character 2'} < {file name}*, where character 1 is the character to be replaced.

The uniq Command

The *uniq* command is used to display unique lines from a sorted file after ignoring successive duplicated lines. Because it compares only consecutive lines, the *uniq* command requires sorted input.

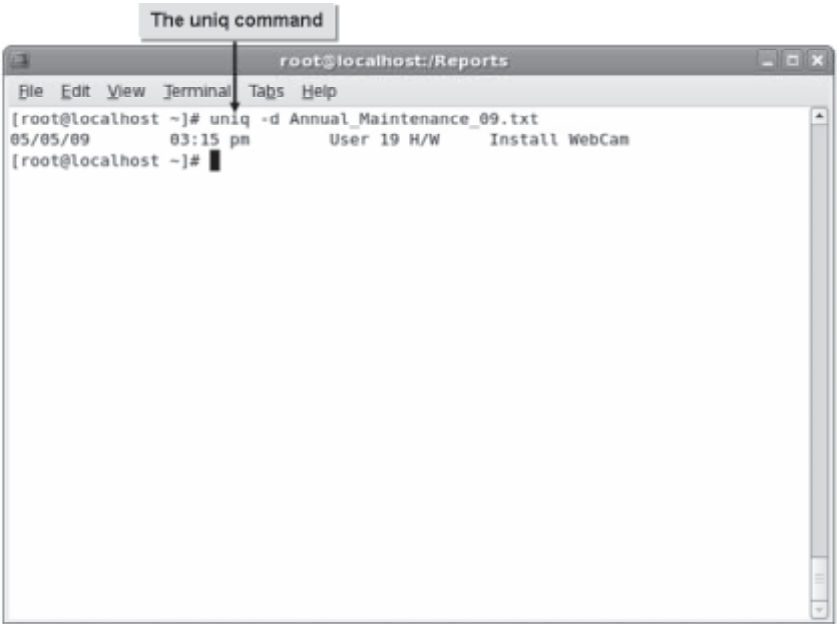


Figure 4-8: Duplicate content displayed using the `uniq` command.

The `uniq` command provides various options that allow you to specify the nature of the output.

Option	Description
<code>-u</code>	Displays only unique lines.
<code>-d</code>	Displays only duplicated lines.
<code>-c</code>	Displays lines prefixed by the number of occurrences.

Syntax

The syntax of the `uniq` command is `uniq [options] {file name}`.

Input and Output Redirection

When you want to redirect the contents of an existing file to another command for processing, the input redirection symbol, less than (`<`), and the output redirection symbol, greater than (`>`), can be used. The output redirection symbol tells the shell to redefine standard output as a file. If the file does not exist, the shell creates it. The input redirection symbol tells the shell to redefine standard input as something other than the keyboard input, usually a file.

For example, the `ls > list` command causes the shell to send the output of the `ls` command to a file named `list`.



Figure 4-9: Redirecting the output of the `ls` command to the `list` file.

How to Create and Edit Files

Procedure Reference: Create a File and Enter Text Using the Vim Editor

To create a file and enter text using the Vim editor:

1. Log in as a user.
2. To create a file, at the command prompt, enter `vim {file name}`.
3. To switch to insert mode, press **I**.
4. Type the required content.
5. To return to command mode, press **Esc**.
6. To save and close the file, enter `:wq`.

Procedure Reference: Create a Text File from the Command Prompt

To create a text file from the command prompt:

1. Log in as a user in either the GUI or the CLI.
2. In the GUI terminal window, or in the CLI terminal, navigate to the directory where you want to create the file. If necessary, create a new directory at the desired location and make it the current directory.
3. At the command prompt, enter `cat > {file name}`.
4. To move to a new line, type the contents of the file and press **Enter**.
5. To save the file and return to the command prompt, press **Ctrl+D**.
6. If necessary, to view the file contents, type `cat {file name}`.

Procedure Reference: Edit Text Files in Vim Command Mode

To edit text files in Vim command mode:

1. Log in as a user.
2. To open a file, enter `vim {file name}`.
3. To make necessary changes, use the appropriate vim shortcuts.
4. To save and close the file, enter `:wq`.

Procedure Reference: Open Multiple Windows Using the vim Command

To open multiple windows using the vim command:

1. Log in as a user.
2. Open multiple windows.
 - To open different files in multiple windows, enter `vim -o {file name 1} {file name 2} ... {file name n}`.
 - To open a new file in a new window, press **Ctrl+W+N**.
 - To navigate through the windows, hold down **Ctrl+W** and use the arrow keys.
3. To make necessary changes, use the appropriate Vim shortcuts.
4. If necessary, to return to command mode, press **Esc**.
5. Save and close the files.
 - To save and close the files one by one, enter `:wq`.
 - Or, to close all files at the same time, enter `:qa`.

Procedure Reference: Count the Words in a File

To count the words in a file:

1. Log in as a user in the CLI.
2. Count the words in a file.
 - To count the number of words, lines, bytes, and characters in the file, enter `wc [options] {file name}`.
 - To count the number of words, lines, bytes, and characters in the output of the command, enter `{command} | wc [options]`.

Procedure Reference: Remove Duplicate and Adjacent Lines in a File

To remove duplicate and adjacent lines in a file:

1. Log in as a user in the CLI.
2. Remove duplicate and adjacent lines in a file.
 - To remove duplicate and adjacent lines from a file, enter `uniq [options] {file name}`.
 - To remove the duplicate and adjacent lines from the output of the command, enter `{command} | uniq [options]`.

Procedure Reference: Compare Files in the CLI

To compare files in the CLI:

1. Log in as a user in the CLI.
2. To compare files for differences in their content, enter `diff {file name 1} {file name 2}`.

Procedure Reference: Compare Files in the GUI

To compare files in the GUI:

1. To switch to the GUI, press **Ctrl+Alt+F7**.
2. From the menu bar, choose **Application**→**Accessories**→**Terminal**.
3. To compare files for differences in content, enter `vimdiff {file name 1} {file name 2}`.
4. To return to the terminal, enter `:q` two times.

Procedure Reference: Replace Characters

To replace characters:

1. Log in as a user in the CLI.
2. Replace characters.
 - To replace one character with another one and display the contents of the file, enter `tr {'character 1'} {'character 2'} < {file name}`.
 - To replace one character with another one from the output of the command, enter `{command} | tr {'character1'} {'character 2'}`.

Working with Multiple Windows

You can choose to tile your windows horizontally or vertically. Press **Ctrl+W+V** to create a vertical split, or press **Ctrl+W+S** to split the screen horizontally.

ACTIVITY 4-1

Creating Text Files Using Vim

Before You Begin:

- 1. You have logged in as root in the CLI.
- 2. The first terminal is displayed.

Scenario:

As a junior system administrator who recently joined OGC, you have several tasks to be completed in a day. Because you are just getting used to your routine tasks, you decide to record the tasks by creating a file named Checklist.txt.

What You Do	How You Do It
1. Create a text file named Checklist.txt.	<ul style="list-style-type: none">a. Enter vim Checklist.txtb. To switch to insert mode, press I.c. Observe that the text "INSERT" is displayed at the bottom-left of the screen.
2. Enter data into the file.	<ul style="list-style-type: none">a. Enter Update Antivirus as the first entry in the file.b. Enter Install New Printer as the second entry.c. Enter Fix Keyboard Issues as the third entry.d. Type Install New Monitor as the fourth and last entry.
3. Save the file in execute mode and exit.	<ul style="list-style-type: none">a. To return to command mode, press Esc.b. To save the file and quit the text editor, enter :wqc. To clear the terminal screen, enter clear

ACTIVITY 4-2

Editing Text Files in Command Mode

Data Files:

- Softwarelist.txt

Before You Begin:

1. You have logged in as root in the CLI.
2. The first terminal is displayed.
3. At the command line, enter `cp /085099Data/Managing_Files/* /root.`
4. Enter `clear.`

Scenario:

Your manager asks you to list the software used in your organization. You list the software in the Softwarelist.txt file. However, before submitting it, you want to ensure that the document is free from errors. You notice the following errors in the document:

- Image Maker appears as Image Marker.
- Photoshop has been entered as photoshop.
- Details about Paintworks have been duplicated.

By resolving these issues, you want to ensure that the document is ready for submission.

What You Do

How You Do It

1. Change the spelling of the text "Image Marker" to "Image Maker."

- a. To open the Softwarelist.txt file, enter **`vim Softwarelist.txt`**
- b. Move the cursor down to the first occurrence of the text "Image Marker Pro."
- c. To move the cursor to the next word, press **W**.
- d. Delete the first occurrence of the letter "r" in the word "Marker."



A warning message may appear at the bottom of the screen stating that the file is read-only. This message can be ignored because the file will ultimately get saved with the changes made to it.

LESSON 4

- | | |
|--|---|
| 2. Fix multiple occurrences of the error. | <ul style="list-style-type: none">a. To search for the next occurrence of the word "Marker," type /Marker and press Enter.b. Change the text "Marker" to "Maker." <hr/> |
| 3. Change the casing of the first letter in "photoshop." | <ul style="list-style-type: none">a. To move to the next line, press J.b. To place the cursor below the first occurrence of the letter "h" in the word "Photoshop," press H.c. To delete the first letter, press C followed by B.d. To change the word to "Photoshop," in insert mode, type Pe. To return to command mode, press Esc. <hr/> |
| 4. Remove the duplicate entry of "Paintworks." | <ul style="list-style-type: none">a. To navigate to the second occurrence of the word "Paintworks," press the Down Arrow key two times.b. To delete the duplicated line, press D two times.c. To save and close the file, enter :wqd. Clear the terminal screen. <hr/> <hr/> |

TOPIC B

Locate Files

In the last topic, you created and edited files. As a user or administrator, you will have to frequently locate files within the Linux filesystem before you can edit them. In this topic, you will locate files within the Linux system.

Learning how to quickly locate files within Linux will reduce the amount of time you spend searching for files. There are different techniques available for locating files within Linux, and these techniques will save you time and effort as you manage larger filesystems.

The locate Command

The *locate* command performs a quick search for any specified string in file names and paths stored in the mlocate database. This database must be updated regularly for the search to be effective. The results displayed may be restricted to files that users have permissions to access or execute.



Figure 4-10: Searching files using the *locate* command.

Syntax

The syntax of the *locate* command is `locate [options] {string}`.

The locate Command Options

The *locate* command supports different options that enable you to make your search more effective. Some of the options are described in the table.

Option	Description
<code>-r</code>	Uses regular expressions in searching for file names.

Option	Description
-c	Displays only the number of matching entries found, rather than the file names.
-e	Returns only files that exist at the time of search.
-i	Ignores the casing in file names or paths.
-n number of entries	Returns only the first few matches up to the specified number.

Updating the mlocate Database

The `updatedb` command is used to build a database of files based on the `/etc/updatedb.conf` file. This command is used to update the `/var/lib/mlocate/mlocate.db` database. The `/etc/updatedb.conf` file consists of the paths that should be excluded while building the database. To add a path that needs to be excluded while building the database, open the `/etc/updatedb.conf` file and, in the `PRUNEPATH` variable, specify the path that need not be included while building the database. For example, `PRUNEPATH="/etc"` will exclude the `/etc` directory while building the database.

Though this is the default database searched by the `locate` command, there may be more databases containing file paths. If the database is not updated before performing a search, all files created after the last update will be excluded from the search.

The slocate Command

The `slocate` command, or secure locate command, searches a specific database that is built using the `slocate -u` command. The difference between the `locate` and `slocate` commands is that when a user types `slocate {file name}`, the `slocate` command searches the database and returns the location of the file only if the user has access permission to those files. The `locate` command, however, returns the location of files whether or not the user has access permission to them.

Using grep

In its simplest form, `grep` is a search tool. It allows you to perform search actions, such as finding any instance you are searching for, in a file. For example, entering `grep foo test` returns all the lines that have a string matching “foo” in the file “test.” The `grep` command can also be used to search a directory for a certain file. The `ls -l | grep audit` command returns a long listing of any files in the current directory whose name contains “audit.”



The term `grep` is derived from “Globally matching a Regular Expression and Printing the lines.”

The whereis Command

The `whereis` command is used to view various details associated with a command. The `whereis` command has various options.

Option	Used To
-b	Search only for binaries.
-m	Search only for manual sections.

Option	Used To
-s	Search only for sources.
-u	Search for unusual entries.



Figure 4-11: The path to the `ls` command.

Syntax

The syntax of the `whereis` command is `whereis [options] [directory] {file name}`.

Using the `whereis` Command

On entering `whereis ls`, the following output is displayed:

```
ls: /bin/ls /usr/share/man/man1/ls.1.gz /usr/share/man/man1p/ls.1p.gz
```

Where `/bin/ls` indicates the location of the `ls` command and `/usr/share/man/man1/ls.1.gz /usr/share/man/man1p/ls.1p.gz` indicates the location of the man pages for the `ls` command.

The GNOME Search Tool

The *GNOME search tool* is a graphical utility used for searching files based on specific criteria. You can search for a file by its name, size, ownership, access time, or contents. This powerful GUI tool supports features such as case-insensitive search, search within a specific location, and wildcard searches. This tool uses a combination of search commands such as `locate`, `find`, and `grep`.

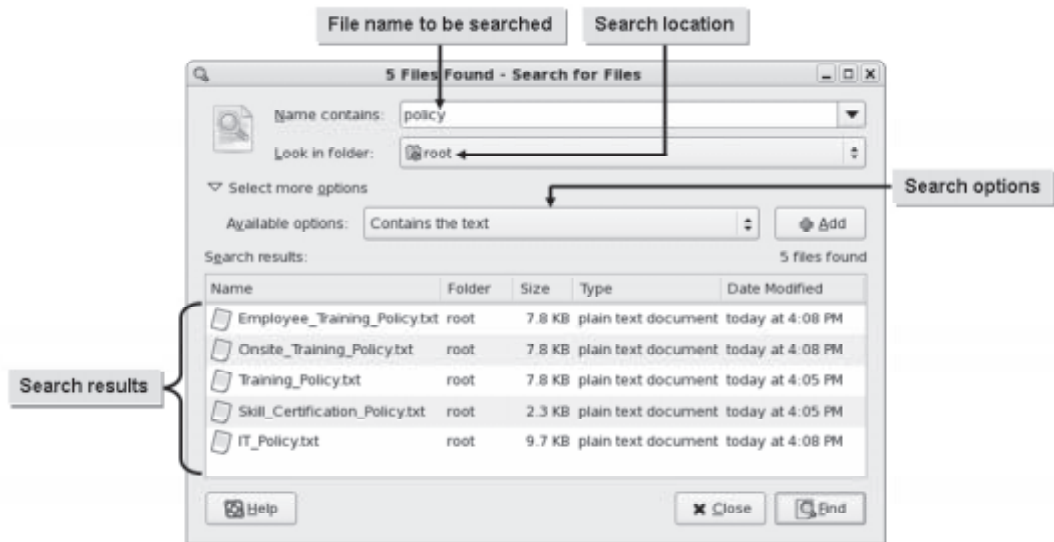


Figure 4-12: Searching files using the GNOME search tool.

Kat

Kat is an application for KDE that is used to search for files with the help of meta information, full text, and thumbnails that are extracted and indexed from various types of files. It serves as a catalog and helps retrieve files quickly.

Beagle

Beagle is a GNOME desktop search application, which can also be used in KDE by installing Kerry. It is used to search for files, folders, documents, notes, images, videos, email messages, instant messaging content, web browser history, and RSS feeds. Beagle indexes files, which enables it to retrieve search results quickly. It also allows users to sort search results based on date modified, name, or relevance.

The find Command

The *find* command enables you to search a specific location for files and directories that adhere to some search criteria. It recursively searches the directory structure, including any subdirectories and their contents, beginning with the search location you enter. You can perform one or more actions on the files found.



Figure 4-13: Searching files using the *find* command.

Syntax

The syntax of the `find` command is `find [options] {search locations} {search criteria} [actions]`.

find vs. locate Commands

The `locate` command searches a database and retrieves information on files present on your system. However, failure to keep this database updated may produce outdated results. The `find` command, on the other hand, performs a live search of the filesystem and may concentrate on a specific location. The `find` command may take more time to complete a search than the `locate` command.

Working of the find Command

You can use the `find` command to search the entire directory structure for a file even if you remember a portion of the file name. One or more search paths can be designated and directory notations can be used as the search path. If no directory is specified, the `find` command uses the current working directory as the location to start the search. One or more criteria can be used to specify the conditions of a file or directory. In case of more than one search criterion, the file or directory must meet all the conditions specified before the results are displayed. The results displayed may be restricted to files users have permissions to access or execute. You can check the manual pages of the `find` command for more options.

Options for Files Found

When the system finds a listing that meets your criteria, there are several actions that can be performed on the results. These options are outlined in the following table.

Option	Action Performed
<code>-print</code>	Displays the location of the files found.

Option	Action Performed
-exec	Executes the command that follows.
-ok	Executes the command that follows interactively.
-delete	Deletes files found.
-fprint	Stores results in the target file.

find Command Conditions

The `find` command can be used with one or more conditions. These conditions accept strings or numbers as arguments.



Figure 4-14: Using the `-name` condition in the `find` command.

Some of the frequently used conditions are listed in the following table.

Condition	Description
-name	Matches by name. Regular expressions may be used as arguments.
-iname	Matches by name, ignoring the case.
-user	Matches by user name or UID of the owner.
-group	Matches by group or GID of the owner group.
-size	Matches by size.
-perm	Matches by symbolic or octal permissions.
-type	Matches by file type.
-newer	Matches by comparing the modification time. Returns files modified later than reference files.
-atime	Matches by access time in days.

Condition	Description
<code>-mtime</code>	Matches by modification time in days.
<code>-ctime</code>	Matches by time of latest changes in a file. Arguments are counted in days.

Logical Operators for Conditions

You can combine conditions using logical operators. When more than one criterion is specified, by default, only those files that satisfy all conditions are returned. However, the logical operator OR can be applied to these conditions by using `-o` between conditions. Also, the NOT operator can be applied to conditions by using `-not` to negate a condition.

Numeric Arguments

Numeric arguments are used to specify a numeric value. The following table lists the numeric arguments for size and their description.

Use This Argument	If You Need To
<code>n</code>	List files that are equal to <code>n</code> units (default option).
<code>+n</code>	List files that are greater than <code>n</code> units.
<code>-n</code>	List files that are less than <code>n</code> units.

The following table lists the numeric arguments for time and their description.

Use This Argument	If You Need To
<code>n</code>	List files that were accessed <code>n</code> days ago (default option).
<code>+n</code>	List files that were accessed more than <code>n</code> days ago.
<code>-n</code>	List files that were accessed less than <code>n</code> days ago.

How to Locate Files

Procedure Reference: Search for Files from the Database

To search for files from the database:

1. Log in as root.
2. To update the `mlocate` database with the file name and path information, enter `updatedb`.
3. To search the updated database for the specified string, enter `locate {string}`.

Procedure Reference: Search for Files Using the GNOME Search Tool

To search for files using the GNOME search tool:

1. Log in as a user in the GUI.
2. To open the search tool, choose **Places**→**Search for Files**.
3. In the Search for Files window, in the **Name contains** text box, type the string to be searched.
4. If necessary, to perform the search, from the **Look in folder** drop-down menu, choose the location.
5. If necessary, to specify additional search criteria such as **Date modified less than**, **Date modified more than**, **Size at least**, **Size at most**, **File is empty**, **Owned by user**, **Owned by group**, **Owner is unrecognized**, **Name does not contain**, **Name matches regular expression**, **Show hidden and backup files**, **Follow symbolic links**, and **Include other filesystems**, click the toggle button beside the text “Select more options.” Click **Add** to add the selected option.
6. If necessary, to view the manual on “Search for Files,” click **Help**.
7. To search for the specified string, click **Find**.

ACTIVITY 4-3

Searching for Files from the Database

Before You Begin:

1. You have logged in as root in the CLI.
2. To navigate to the Server directory, on the terminal, enter `cd /rhelsource/Server`.
3. If necessary, to install the kernel-headers package, enter `rpm -ivh kernel-headers*`.
4. To clear the terminal screen, enter `clear`.

Scenario:

You are required to make a report of all peripherals purchased in the past few years, to calculate further requirements. You want the details of all software licenses purchased by the organization. To locate the files and directories containing this information, you decide to perform a local search for the term “software.”

What You Do

How You Do It

1. Search the database for filenames containing the word "software."

- a. To update the mlocate database, enter **updatedb**



This may take a few minutes. Please wait until the update is complete and the shell prompt reappears.

- b. To search for all files containing "software" in their name, enter **locate -i *software***

- c. Observe that all files, including system files, that contain "software" in their names are listed.

2. Ensure that all directory names containing the word "software" are listed.

- a. To switch to the root directory, enter **cd /**

- b. To search all path names containing the term "software," enter **ls -lR | grep -i "software" | more**

- c. To check for any directories containing the term "software" in their name, press the **Spacebar** until you reach the end of the list.

- d. Observe that the software directory under **/usr/src/kernels/2.6.18-128.el5-i686/include/config** is displayed in the result.

- e. To clear the terminal screen, enter **clear**

ACTIVITY 4-4

Searching for Files in the GUI

Before You Begin:

- 1. You have logged in as root in the CLI.
- 2. To change the ownership, on the terminal, enter `chown -R jsmith /085099Data/Locating_Files/*`.
- 3. To create the `work_files` directory, enter `mkdir /work_files`.
- 4. To copy the files, enter `cp -pR /085099Data/Locating_Files/* /work_files`.
- 5. To clear the terminal screen, enter `clear`.

Scenario:

As a system administrator, it is your responsibility to perform a regular system cleanup. You want to clear all the unnecessary empty files. You decide to search for empty files on the Linux filesystem to mark them for deletion.

What You Do	How You Do It
1. Open the GNOME search tool.	<ul style="list-style-type: none">a. Switch to the GUI.b. Log in as root.c. To open the GNOME search tool, choose Places→Search for Files.
2. Specify the search location as the <code>/work_files</code> directory.	<ul style="list-style-type: none">a. To include all files for the search, in the Search for Files dialog box, in the Name contains text box, type <code>*</code>b. To open the Browse window, from the Look in folder drop-down menu, select Other.c. To display more destination directories in the right pane, in the Places list box, double-click File System.d. To view more directories, in the Browse dialog box, in the Name list box, scroll down.e. To select the <code>/work_files</code> directory and exit the window, in the Name list box, select work_files and click Open.

3. Search for empty files.
 - a. Click the toggle button beside the text "Select more options" to display more search options.
 - b. To restrict the search results to empty files, from the **Available options** drop-down list, select **File is empty** and click **Add**.
 - c. To search for empty files within the /work_files directory, click **Find**.
 - d. Maximize the window and scroll down to observe all the empty files listed.
 - e. To close the Search for Files window, click **Close**.
-

TOPIC C

Search Text Using Regular Expressions

In the last topic, you located files within the Linux system. In Linux, you can search text files by specifying a particular portion of text or even just some characters of the file. You can then make the desired modifications to these characters. In this topic, you will search text files to locate text and characters.

Consider that you have created a new text file and that there are pages of content within it. Now, you discover that you need to modify a particular word. Going through lines and lines of text to locate one word is a daunting task. Using the plain text search option will also be time consuming. It would be much easier if you can locate a particular word with a few simple keystrokes, and this is where regular expressions can help.

Regular Expressions

Definition:

Regular expressions are strings of characters that denote a word, a set of words, or a sentence. They describe a pattern for searching. Locating text, replacing text, and manipulating strings are the main uses of regular expressions.

Example: A Regular Expression

To copy all the files that end in ".html", `cp *.html .. /` is used.

Expressions

Expressions are a group of characters. They are formed by combining variables and constants with operators. They are used in `if` and `while` statements. Performing arithmetic comparisons, string comparisons, and testing files are the main functions of expressions. If an expression contains the `<`, `>`, `&`, or `!` symbols, parentheses are required.

How to Search Text Files Using Regular Expressions

Procedure Reference: Search Using the Regular Expression Tool

To search using the regular expression tool:

1. Log in as root in the CLI.
2. Search using the regular expression tool.
 - To search through a filesystem using the regular expression tool, enter `ls -l | grep -{options} {regular expression with notational elements}`.
 - To search through a file content using the regular expression tool, enter `grep -{options} {regular expression with notational elements} {file name}`.

Regular Expression with Notational Elements

A regular expression with notational elements is a search string formed by combining wildcards, numbers, and characters.

For example, `[^e]?b[1-9]` as a whole is called a regular expression with notational elements, where the notational elements are `^`, `?`, and `[1-9]`. This expression searches for a file/word/ directory that starts with the letter “e” followed by a character/number, then by the letter “b”, and finally by a number ranging between 1 and 9.

Another example of a regular expression with notational elements is `1\{5\}`, where `\{` and `\}` are the notational elements. This expression searches for the occurrence of the number “1” repeated consecutively five times. Regular expression is often referred to as `regex`.

ACTIVITY 4-5

Searching Text Files

Data Files:

- Leave_Log.txt

Before You Begin:

1. You have logged in as root in the GUI.
2. Switch to the CLI.
3. To change to the /root directory, enter `cd /root`.
4. To create a new directory, enter `mkdir HR`.
5. To copy the data file, enter
`cp /085099Data/Managing_Files/Leave_Log.txt /root/HR`.
6. To clear the terminal screen, enter `clear`.

Scenario:

An HR employee in your organization wants to collect the following leave details, for the month of January, for all employees from the software and network departments:

- Employees from the network department who have taken sick leave.
- Employees from the software department who were awarded compensatory leave.
- Employees who have gone on vacation from both the departments.

Because the Leave_Log file, located in the HR directory, has many details, the HR employee finds it difficult to manually go through the file and collect the details. You need to get the specified details using the department and leave identification codes given below.

- Employee code for the software department: 000
- Employee code for the network department: 111
- Sick leave: SL
- Compensatory leave: Comp
- Vacation: VC

LESSON 4

What You Do	How You Do It
1. Find all employees in the network department who have taken sick leave.	<ol style="list-style-type: none">To change the directory, enter cd HRTo view the contents of the file, enter cat Leave_Log.txtObserve that the contents of the file are displayed on the screen.To clear the terminal screen, enter clearTo list all the network department employees who have taken leave, enter grep -i '1\{3\}' Leave_Log.txtObserve that the list of all the network department employees who have taken leave are displayed on the screen.To list all the network department employees who have taken sick leave, enter grep -i '1\{3\}.*SL'⇒ Leave_Log.txtObserve that the list of all the network department employees who have taken sick leave are displayed on the screen.Clear the terminal screen.
2. List all employees who have gone on vacation.	<ol style="list-style-type: none">To list all the employees gone on vacation, enter grep -i 'VC' Leave_Log.txtObserve that the list of all employees who have gone on vacation are displayed on the screen.Clear the terminal screen.

3. List the employees of the software department who have been awarded compensatory leave.
 - a. To list all the software department employees who have taken leave, enter `grep -i '0\{3\}' Leave_Log.txt`
 - b. Observe that the list of all the software department employees who have taken leave are displayed on the screen.
 - c. To list all the software department employees who have been awarded compensatory leave, enter `grep -i '0\{3\}.*Comp' Leave_Log.txt`
 - d. Observe that the list of all the software department employees who have been awarded compensatory leave are displayed on the screen.
 - e. Clear the terminal screen.
-

TOPIC D

Apply Filters to Text Streams

In the previous topic, you used regular expressions to locate text in files. In the course of your work, it will prove helpful if you can break the entire text into logical groups that match certain patterns. This will be useful when you want to make changes that affect some, but not all, data. In this topic, you will apply filters to text streams to break them into sections that match specific criteria.

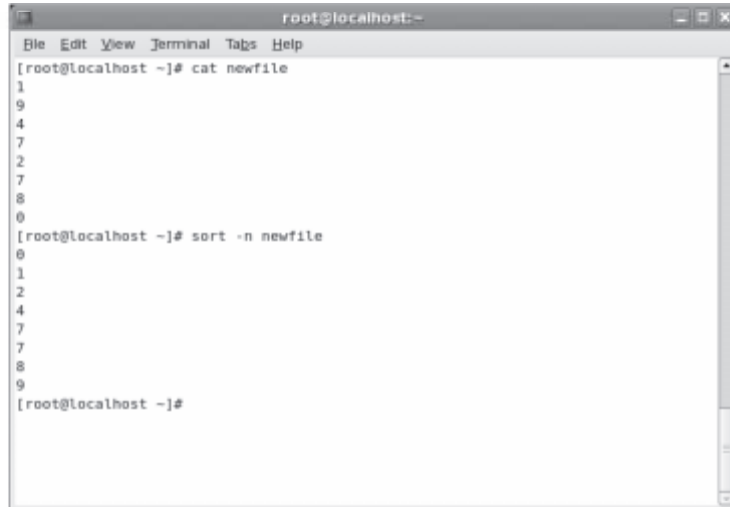
Imagine a scenario where a merger takes place between two organizations. Merging and sorting select policy documents and employee databases can be a tedious task for an administrator. Applying filters makes the task of merging these documents and sorting the employee database an easy one.

Filters

Definition:

A *filter* is a program that accepts an input or output request, verifies what data matches the criterion specified in the request, and then processes it. Filters are shell scripts and are sometimes used to insert or remove headers.

Example: Setting a Filter



```

root@localhost:~# cat newfile
1
9
4
7
2
7
8
0
root@localhost:~# sort -n newfile
0
1
2
4
7
7
8
9
root@localhost:~#
  
```

Figure 4-15: Sorted output of a file.

Text Streams

Definition:

A *text stream* is a sequence of one or more lines of text that can be written to be read on a text-based display. While reading from or writing to a text stream, the program divides the data into lines by reading an NL, or newline, at the end of each line.

Example:

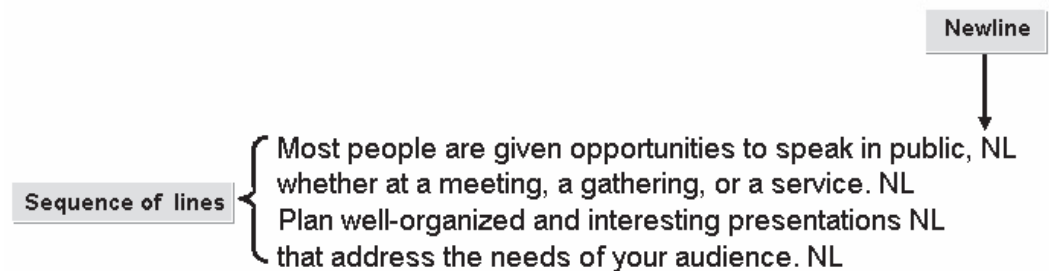


Figure 4-16: Sequence of lines that use the NL character.

Limitations of Text Streams

The position of the text stream should not be changed while reading from or writing to it. Depending on the kind of text file being used, text streams may not support all character values.

How to Apply Filters to Text Streams

Procedure Reference: Modify Output Using the join Command

To modify the output of text files using the `join` command:

1. If necessary, navigate to the relevant directory.

2. To join the two files by their first column content followed by the rest of the columns, provided the first columns of the files are identical on the standard output, enter `join {file name 1} {file name 2}`.
3. If necessary, to join the two files and redirect the output to a file, enter `join {file name 1} {file name 2} > {file name}`.



While using the `redirect` command, you may generate additional files. For example, when you use multiple `textutil` commands to generate the desired output, you may redirect the content from one file to another, thereby generating additional files. You may want to delete these unwanted files to avoid confusion.

Procedure Reference: Send Output Streams of the `cut` Command Through the `sort` Command

To modify output by directing the output stream of the `cut` command through the `sort` command:

1. If necessary, navigate to the relevant directory.
2. To send the output streams of the `cut` command through the `sort` command, enter `cut {options} {delimiter} -{field number}{file name} | sort {options}`.

The `cut` Command Options

The `cut` command cuts out the selected columns or fields. Common `cut` command options and their uses are given in the following table.

If You Need To	Use This <code>cut</code> Command Option
Delimit one field from another field.	<code>-d={delimiter}</code>
Suppress a line if the delimiter is not found.	<code>-s</code>
Specify the field number. For example, <code>f2</code> indicates the second field.	<code>-f={column number / column list}</code>

Delimiter

A delimiter can be a tab, space, colon, semicolon, period, or comma used to separate one field from another.

The `sort` Command Options

The `sort` command arranges the lines in a file. Common `sort` command options and their uses are given in the following table.

If You Need To	Use This <code>sort</code> Command Option
Specify field values. For example, <code>-k2</code> indicates the second field.	<code>-k={column number}</code>
Compare and sort lines based on the string numerical value.	<code>-n</code>

If You Need To	Use This <code>sort</code> Command Option
Sort fields in descending order. Note: By default the fields are sorted in ascending order.	<code>-r</code>
Separate one field from another.	<code>-t={delimiter}</code>

Textutil Commands

Textutil commands are used to modify an output. Some common textutil commands and their description are given in the following table.

If You Need To	Use This Textutil Command
Convert tabs in a file to appropriate number of spaces.	<code>expand {file name}</code>
Format text to a specified width by filling empty lines for the specified file name.	<code>fmt {file name}</code>
Display the first 10 lines of a file.	<code>head {file name}</code>
Count the number of lines in a file.	<code>nl {file name}</code>
Dump the specified files in octal format.	<code>od {file name}</code>
Merge lines of one or more files.	<code>paste {one or more files}</code>
Convert a text file to print.	<code>pr {file name}</code>
Split a file into equally sized pieces.	<code>split {file name}</code>
Display files in reverse to the standard output.	<code>tac {file name}</code>
Display the last 10 lines of a file.	<code>tail {file name}</code>
Translate characters from one format to another and to the standard output.	<code>tr {one format} {another format}</code>
Convert white spaces to appropriate number of tabs for the specified file name.	<code>unexpand {file name}</code>
Delete duplicate adjacent lines from a sorted file.	<code>uniq {file name}</code>
Print the byte, word, and line counts of the specified file name.	<code>wc {file name}</code>

ACTIVITY 4-6

Applying Textutil Commands to Modify the Output

Data Files:

- Empclaimfeb.txt
- Empclaimjan.txt


Before You Begin:

1. You have logged in as root in the CLI.
2. To copy the data files, enter
`cp /085099Data/Managing_Files/Empclaim*.txt /root/HR.`
3. To clear the terminal screen, enter `clear`.

Scenario:

Mike, a colleague in the finance department, wants to create a consolidated bimonthly report for claims submitted by employees. This report would be for the months of January and February, sorted by employee number. You will help Mike in creating the consolidated report.

The consolidated report should be named Empclaim.txt.

What You Do	How You Do It
1. Join the Empclaimjan.txt and Empclaimfeb.txt files to create a consolidated report named empclaims.txt.	<ol style="list-style-type: none"> Enter <pre>join Empclaimjan.txt Empclaimfeb.txt⇒ > empclaims.txt</pre> <div data-bbox="756 1178 797 1226"></div> <p>The ⇒ symbol indicates that the text appearing on the next line should be typed on the same line in which ⇒ appears.</p> Enter <code>cat empclaims.txt</code> Observe that the contents of the file are displayed on the screen. Enter <code>clear</code>

LESSON 4

2. Sort fields based on the employee number.
 - a. To sort the empclaims.txt file in ascending order of the **EmployeeNumber** field and redirect the sorted output to the Empclaim.txt file, enter

```
sort -n empclaims.txt > Empclaim.txt
```
 - b. To view the contents of the file, enter

```
cat Empclaim.txt
```
 - c. Observe that the contents of the file are sorted in ascending order of the **EmployeeNumber** field.
 - d. To clear the terminal screen, enter **clear**

3. Delete unwanted files from the HR directory.
 - a. To remove the three files, enter **rm empclaims.txt Empclaimjan.txt Empclaimfeb.txt**
 - b. To delete all the files, enter **y** three times.
 - c. To verify that the files are deleted, enter **ls**
 - d. Observe that only the Empclaim.txt and Leave_Log.txt files are listed, which indicates that the other three files are deleted.
 - e. To clear the terminal screen, enter **clear**

TOPIC E


Link Files


You know how to locate files within the Linux system. Creating a link or shortcut to those files will enable you to locate them easily. In this topic, you will link files in Linux.

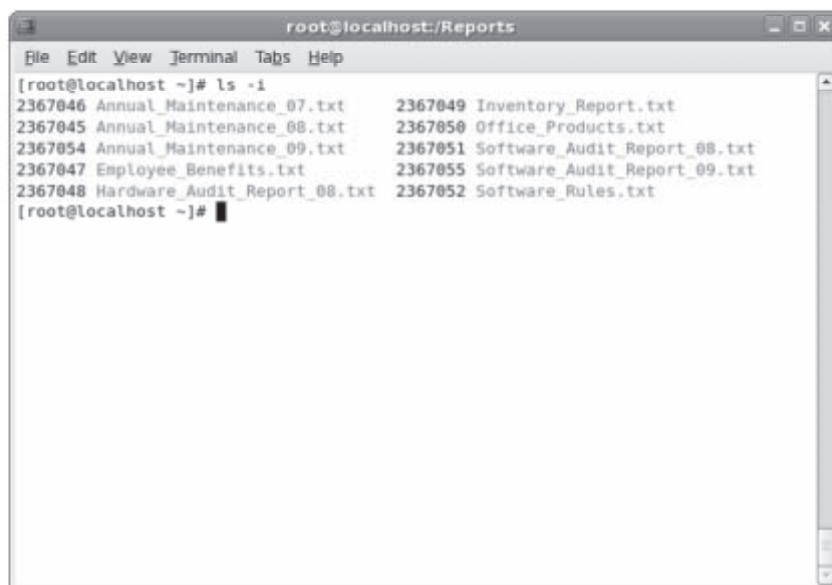
Linking files within Linux will help you track frequently used files without having to navigate through the file structure to search for them each time. You can help users who are not familiar with Linux to access related files by linking the files.

Inodes

An *index node (inode)* is a computer's reference for a file. The *index node table*, or inode table, is a data structure that contains information about individual files in a filesystem. Inode is an entry in the table that contains information about the device where the inode resides, the file type, the mode of file, and the UID and GID of the owner. It also contains information about the number of links to the file, the number of bytes in the file, the time of access and modifications, the time when the inode itself was last modified, and the addresses of the file's blocks on the hard disk. The `ls -li` command is used to locate the inode number of a file.

 In the debugfs utility interface, you can use the `ffi` command to find free inodes.

 Based on permissions, file modes can be writable, readable, or executable. The `chmod` command allows you to modify permissions for a file.



```
root@localhost:/Reports
File Edit View Terminal Tabs Help
[root@localhost ~]# ls -li
2367046 Annual_Maintenance_07.txt      2367049 Inventory_Report.txt
2367045 Annual_Maintenance_08.txt      2367050 Office_Products.txt
2367054 Annual_Maintenance_09.txt      2367051 Software_Audit_Report_08.txt
2367047 Employee_Benefits.txt          2367055 Software_Audit_Report_09.txt
2367048 Hardware_Audit_Report_08.txt   2367052 Software_Rules.txt
[root@localhost ~]#
```

Figure 4-17: Files listed with inode numbers.

The ln Command

The *ln* command is used to create a link to a file. A link allows a file name in one directory to point to a file in another directory. A link does not contain data of its own, only a reference to another file. Any changes to the link will reflect in the original file.

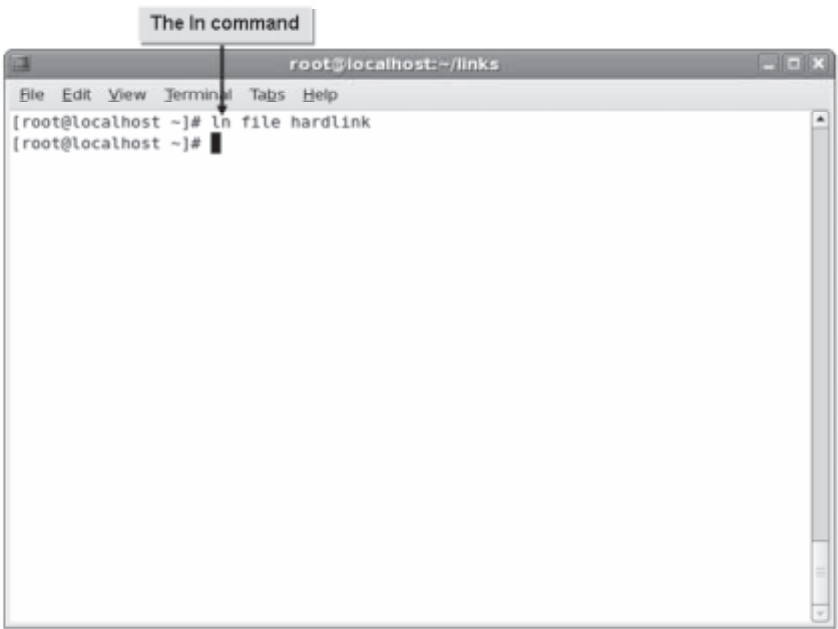


Figure 4-18: A link created using the *ln* command.

Syntax

The syntax of the *ln* command is `ln [option] {target} {link name}`.

In Command Options

The *ln* command has various options. Some of the frequently used options are given in the following table.

Option	Used To
--backup	Back up existing destination files.
-f	Remove existing destination files.
-s	Make symbolic links instead of hard links.
-i	Prompt to remove destination files.
-v	Print the name of a file before linking.

Types of Links

Using the *ln* command, you can create two types of links: hard and symbolic.

Link	Description
<i>Hard</i>	A hard link is a reference to another file; it allows the file's data to have more than one name in different locations in the same filesystem. Applications treat a hard link as a real file. If the original file is deleted after a hard link is created, all its contents will still be available in the linked file. Hard links cannot be created between two directories, nor can they be created between two files in different filesystems.
<i>Symbolic</i>	A symbolic link is a reference to a file or directory that allows you to access mounted filesystems from a different directory. Unlike hard links, symbolic links can be created between two filesystems. If the original file is deleted after a symbolic link is created, then the original content is lost. A symbolic link is also known as a soft link.

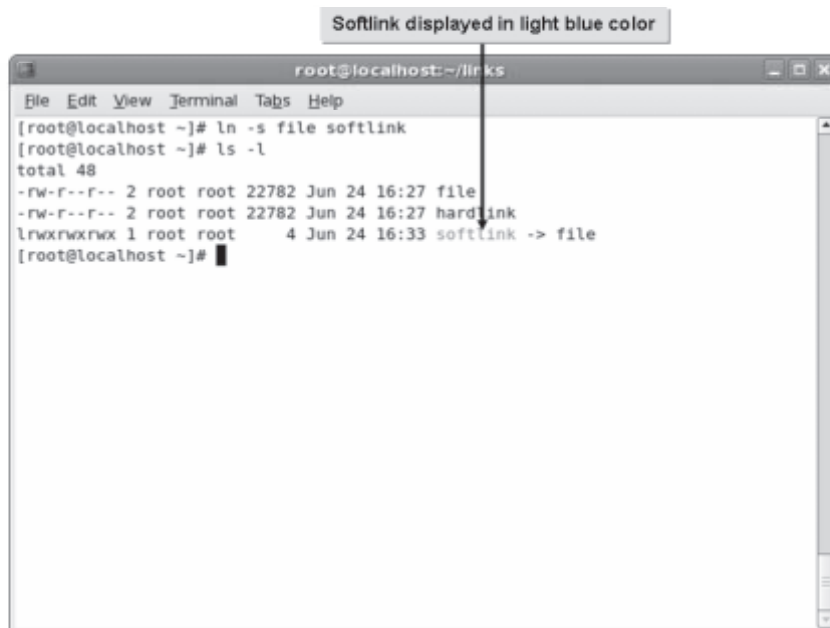



Figure 4-19: A hard link and soft link created for the same file.

 Hard and soft links are a feature of the ext2 filesystem and are common in filesystems of most Unix and Unix-like operating systems such as Linux.

How to Link Files

Procedure Reference: View the Inode Number of a File or Directory

To view the inode number of a file or directory:

1. Log in as a user in the CLI.
2. To view the inode details, enter `ls -li {file or directory name}`.

Procedure Reference: Link Files


To link files:

1. Log in as a user in the CLI.
2. Create file links.
 - To create a hard link, enter `ln {source file} {destination file}`.
 - To create a soft link, enter `ln -s {source file} {destination file}`.
3. To view the inodes of the file, enter `ls -i {file name}`.

Procedure Reference: Copy Files Through Links

To copy a file through a link:

1. Log in as root in the CLI and navigate to the relevant directory.
2. To create a symbolic link, enter `ln -s {file/directory name} {link name}`.

 A symbolic link is indicated by the name of the link in light blue color and an arrow pointing to the source file.
3. To copy the file through a symbolic link, enter `cp {link name} {target name}`.
4. If necessary, to check if the file has been copied, enter `ls -l`.

Procedure Reference: Use Linked Files to Support System Administration Tasks

To create links to files that support system administration tasks:

1. Log in as root in the CLI and navigate to the relevant directory.
2. To create a symbolic link for a system task, enter `ln -s {system file} {link name with path}`.
3. If necessary, to execute the system file, enter `{link name}`.

ACTIVITY 4-7

Linking Files

Data Files:

- Audit_File_09
- Software_List.txt
- New_Policies.txt

Scenario:

You have been assigned the task of reviewing an updated employee policy document for casing errors, making a word count of the document, and creating links of the document as a backup in your local system. You also want to clean up your system by removing unused files from your current working directory and back up the policy document.

What You Do	How You Do It
1. List the files in the current working directory.	<div>a. To change the directory, enter <code>cd /root</code></div> <div>b. To list the files in the directory, enter <code>ls -l</code></div> <div>c. Observe that all the files in the current working directory are listed.</div>
2. Move the Audit_File_09 file to the /jsmith directory and remove the Software_List.txt file.	<div>a. To move the audit file to the /jsmith directory, enter <code>mv -v Audit_File_09 /home/jsmith</code></div> <div>b. To verify that the file transfer is complete, enter <code>ls -l /home/jsmith</code></div> <div>c. To remove the software file from the /root directory, enter <code>rm Software_List.txt</code></div> <div>d. To confirm the deletion, type <code>y</code> and press <code>Enter</code>.</div> <div>e. To check whether the file is deleted, enter <code>ls</code></div> <div>f. Observe that the Software_List.txt file has been deleted.</div>

LESSON 4

3. Edit the `New_Policies.txt` file for casing errors and generate the word count.
 - a. To view the contents of the file, enter **`cat New_Policies.txt`**
 - b. Observe that casing of the letter "Y" in the word "Empl`o`Yees" is incorrect.
 - c. To change the casing of the letter "Y" in the word "Empl`o`Yees" in the output, enter **`tr 'Y' 'y' < New_Policies.txt`**
 - d. Observe that the casing of the letter "Y" has changed in the output.
 - e. To count the words in the file, enter **`wc -w New_Policies.txt`**
 - f. Observe that the word count of the file is displayed.

4. Create a hard link for the file.
 - a. To create a hard link for the file, enter **`ln New_Policies.txt New_Policies_09.txt`**
 - b. To view whether the hard link has been created, enter **`ls New*`**
 - c. Observe that the hard link is created.
 - d. Clear the terminal screen.

ACTIVITY 4-8

Creating Links to Frequently Used Files

Data Files:

- Attendancelogfile.txt
- Currentdatetime

Before You Begin:

1. You have logged in as root in the CLI and the first terminal is displayed.
2. To copy the data file, enter
`cp /085099Data/Managing_Files/Attendancelogfile.txt /opt.`
3. To copy the data file, enter
`cp /085099Data/Managing_Files/Currentdatetime /opt.`
4. To modify the file to make it an executable file, enter `chmod +x /opt/Currentdatetime.`
5. To clear the terminal screen, enter `clear.`

Scenario:

You would like to add hard links to files that you use frequently. Both files are located in the /opt directory. One of the files is a text file and the other is an executable program. You have to make these files easily accessible from the root directory without disturbing their original location.

What You Do

How You Do It

1. **True or False? When you delete a hard link, the file to which the hard link is set will also get deleted.**
☐ True
☐ False
2. Create a hard link named "attlog" in the root directory for the Attendancelogfile.txt file located in the /opt directory.
 - a. To create a hard link, enter `ln /opt/Attendancelogfile.txt⇒ attlog`
 - b. To view the hard link, enter `ls -l attlog`
3. **True or False? If an executable file is located in the search path, then the user can run the file from any location.**
☐ True
☐ False

4. Create a symbolic link named "Time" for the executable program, Currentdatetime, located in the /opt directory.
 - a. To create a soft link, enter

```
ln -s /opt/Currentdatetime⇒  
/bin/Time
```
 - b. To view the soft link, enter `ls -l /bin/Time`
 - c. To execute the file, enter `Time`
 - d. To clear the terminal screen, enter `clear`
-
-

TOPIC F

Back Up and Restore Files

In the previous topics, you created, edited, located, and linked files. It is essential that you also know how to back up and restore these files when the need arises. In this topic, you will back up and restore files.

Learning how to back up and restore files will save you countless hours of repairing your system after a system failure. Backing up and restoring files allow you to keep an additional copy of files on your system because they existed at a specific point in time. If you ever have a system failure, these files can be used to restore your system.

Archiving

Definition:

Archiving is a method of storing data by copying data from a system disk drive into a backup device. This is done to preserve a record of the data for future reference or to create data dumps. In the event of a network disruption resulting in data loss, the data can be retrieved from archives.

Example:

Built-in tool to perform archive operations

```

root@localhost:~# dump -0a -f /dev/st0 /usr/src
DUMP: Date of this level 0 dump: Sun Jun  6 17:01:12 2010
DUMP: Dumping /dev/mapper/VolGroup00-LogVol00 (/ (dir usr/src)) to /dev/st0
DUMP: Label: none
DUMP: Writing 10 Kilobyte records
DUMP: mapping (Pass I) [regular files]
DUMP: mapping (Pass II) [directories]
DUMP: estimated 36684 blocks.
DUMP: Volume 1 started with block 1 at: Sun Jun  6 17:01:13 2010
DUMP: dumping (Pass III) [directories]
DUMP: dumping (Pass IV) [regular files]
DUMP: Closing /dev/st0
DUMP: Volume 1 completed at: Sun Jun  6 17:01:24 2010
DUMP: Volume 1 70690 blocks (69.03MB)
DUMP: Volume 1 took 0:00:11
DUMP: Volume 1 transfer rate: 6426 kB/s
DUMP: 70690 blocks (69.03MB) on 1 volume(s)
DUMP: finished in 11 seconds, throughput 6426 kBytes/sec
DUMP: Date of this level 0 dump: Sun Jun  6 17:01:12 2010
DUMP: Date this dump completed: Sun Jun  6 17:01:24 2010
DUMP: Average transfer rate: 6426 kB/s
DUMP: DUMP IS DONE
root@localhost ~#
  
```

Figure 4-20: Archiving files using the *dump* command.

The cpio Command

The *cpio* command copies files to and from archives. It is included in standard Linux distributions. The *cpio* command has three operating modes.

Operating Mode	Description
Copy-out <i>cpio -o</i>	In this mode, the command copies files into an archive. It reads the standard input to obtain a list of file names and then copies those files to the standard output.
Copy-in <i>cpio -i</i>	In this mode, the command copies files from an archive. It extracts files from the standard input.
Copy-pass <i>cpio -p</i>	In this mode, the command copies files from one directory tree to another. It reads the standard input to obtain the list of file names that are created and copied into the destination directory.

The dd Command

The *dd* command copies and converts files to enable them to be transferred from one type of media to another. The *dd* command has various options.



A selected input file is copied to a selected output file. If no files are selected, the standard input and the standard output are used.

Option	Used To
<code>if={file name}</code>	Specify the file from which data will be read.
<code>of={file name}</code>	Specify the file to which data will be written.
<code>bs={number of bytes per block}</code>	Specify the number of bytes at which data is read from an input file and written to an output file.
<code>count={number of blocks}</code>	Specify the number of blocks to be written to the output file from the input file.

Syntax

The syntax of the `dd` command is `dd [operand]... or dd [option]`.

The dump Command

The *dump* command dumps all files in a filesystem into a tape or another file. It can also be used to dump files modified after a specified date. The `dump` command has various options.

Some of the common `dump` command options are provided in the following table.

Option	Used To
<code>-0</code>	Make a full backup.
<code>-1 to 9</code>	Make incremental or partial backups.
<code>-b {maximum block size}</code>	Specify the number of kilobytes per dump record.
<code>-f {location of the target file}</code>	Specify the target location.
<code>-z{compression level}</code>	Specify the compression level in the range 1 to 9.

Syntax

The syntax of the `dump` command is `dump {-level #} -f {file} {filesystem/file/directory}`.

The tar Command

The *tar* command allows you to create archives of data. You can use the command on previously created archives to extract files, store additional files, update files, and list files that were already stored. The `tar` command can also direct its output to available devices, files, or other programs using pipes.

 `tar` is derived from Tape ARchive.



Figure 4-21: Archiving files using the tar command.

Syntax

The syntax of the tar command is `tar [options] {source file} {destination file}`.

The gzip Command

GNU zip (gzip) is a compressing utility that reduces the size of selected files. The gzip command has several options.

These command options are described in the following table.

Option	Description
-d	Decompresses the file.
-f	Forces compression or decompression of a file even if it has multiple links or if the file exists.
-h	Displays a help screen.
-L	Displays the gzip license.
-n	Omits saving the original file name and time stamp.
-N	Saves the original file name and time stamp.
-q	Suppresses all warnings.
-r	Descends into the directory and compresses files.
-v	Displays the name and percentage reduction of the compressed or decompressed file.
-t	Checks the compressed file for integrity.

Syntax

The syntax of the `gzip` command is `gzip [options] {file name}`.

File Compression Utilities

File compression utilities, such as `gzip`, attempt to compress only regular files and ignore symbolic links. Compressed files can be restored to their original form using `gzip -d`, `gunzip`, or `zcat`. If the original file name saved in the compressed file is not suitable for its filesystem, a new name is provided from the original one.

File Archiving Utilities

Various file archiving utilities enable you to compress, decompress, and run other text-processing utilities on files. Some of the utilities are described in the following table.

Utility	Description
<code>bzip2</code>	Compresses files at a faster rate than the <code>gzip</code> command. The syntax of this command is <code>bzip2 {file name}</code> .
<code>bunzip2</code>	Decompresses files that are compressed using the <code>bzip2</code> command. The syntax of this command is <code>bunzip2 {file name}</code> .
<code>bzcat</code>	Decompresses files that are compressed using the <code>bzip2</code> command to the standard output. The syntax of this command is <code>bzcat {file name}</code> .
<code>bzdiff</code>	Runs the <code>diff</code> command on compressed files. The syntax of this command is <code>bzdiff {file name}</code> .
<code>bzip2recover</code>	Recovers data from damaged <code>bzip2</code> files. The syntax of this command is <code>bzip2recover {file name}</code> .
<code>bzless</code>	Runs the <code>less</code> command on compressed files. The syntax of this command is <code>bzless {file name}</code> .
<code>bzmore</code>	Runs the <code>more</code> command on compressed files. The syntax of this command is <code>bzmore {file name}</code> .

 `bzip` is a compression utility currently replaced by `bzip2`.

The unzip Command

The `unzip` command is used to list, test, and extract compressed files in a ZIP archive. The `unzip` command comprises various options.

A few of these options are described in the following table.

Option	Description
-c	Extracts files to the standard output.
-t	Tests files before extraction.
-f	Extracts new files and freshens existing files.
-z	Displays the archive comment.
-v	Extracts and lists files in a verbose manner.



The `unzip` command extracts all files from the specified ZIP archive into the current working directory.

Syntax

The syntax of the `unzip` command is `unzip [options] {file name} -d [directory]`.

Guidelines to Determine a Backup Strategy

An effective backup strategy provides a quick and effortless recovery, minimizing the loss of data in the event of an unexpected crisis.

Guidelines:

To choose an effective backup strategy, follow these guidelines:

- Determine the scope of the backup operation to be performed.
 - Do you need to back up data on a single computer?
 - Do you need to back up data on multiple computers?
 - Are the computers situated in a single location?
 - Are the computers spread across different locations?
- Make sure that you have all the necessary information about the data to be backed up.
 - Identify the amount of data that needs to be backed up.
 - Does the data reside on a single system?
 - Is the data distributed among several servers?
 - Can the data be easily replaced?
- Determine the most suitable time for performing backup operations so that users can continue working.
- Ensure that users are informed well in advance about scheduled backups.
- Review the storage space.
 - Do you have an adequate number of storage tapes?
 - Determine the reliability of the backup media.
 - Determine whether the previous backup versions can be erased or not. It is advisable to retain previous backup versions.
- Depending on the scope of the backup operation to be performed, determine if you have the required number of human resources to perform the backup operation.

- Test the backup operations performed and verify the integrity of the backed up files.

Example: A Good Backup Strategy

A major corporation, OGC, recently suffered a catastrophic loss of data during a power outage caused by a snowstorm. As a preventive measure, the system administrator, Larry, decides to update the organization's backup strategy. To begin with, he notices that team members regularly save work-in-progress files on their local hard drives. He also determines where the other mission critical files are stored. Based on these findings, Larry creates a backup plan that includes all computers on the network. He reviews the storage capacity of the current backup media, and finds it to be inadequate. After some research, he recommends to management that a new storage system be purchased and installed. Finally, Larry consults various managers and team leads to determine the teams' work schedules. He schedules backups from 10:00 P.M.-4:30 A.M., when there will be minimal disruption.

motd

The *message of the day* (*motd*) file is displayed to all users on a daily basis and can be used to inform users about scheduled backups. It requires less disk space than email messages. The contents of the */etc/motd* file are displayed after a user successfully logs in.

The Hanoi Sequence

While performing incremental or partial backups, the Hanoi sequence helps minimize the number of tapes used. Backup procedures have several levels ranging from 0-9. Level 0 indicates a complete backup and ensures that the entire filesystem is copied. A level number greater than 0 indicates that all new files and files modified since the last backup of the same or lower level will be copied. This is known as an incremental backup.

It is practical to always start with a level 0 backup. A level 0 backup should be performed at regular intervals, preferably once a month or once every two months. Data should be stored in a set of fresh tapes each time a level 0 backup is performed. These tapes should be stored forever. After performing a level 0 backup, dumps of active filesystems need to be made on a daily basis. A modified "Tower of Hanoi" algorithm is used for this purpose. The sequence of dump levels followed in this method is 3 2 5 4 7 6 9 8 9 9.

Every week, a level 1 dump needs to be taken and the daily Hanoi sequence repeats beginning with a dump level of 3.

The */etc/issue* and */etc/issue.net* Files

The */etc/issue.net* file is the login banner that users see when they make a network connection with the system. For example, when you use a command line tool to connect with a system, the content in the */etc/issue.net* file is displayed. It includes all the welcome information text displayed whenever a new session is opened. The */etc/issue* and the */etc/issue.net* files constitute the login banner that is displayed to local users. The */etc/issue* file can be customized.

The restore Command

The *restore* command enables you to restore files or filesystems from backups made using the *dump* command. This command can be used across networks to restore data.

The following table describes common `restore` command options.

Option	Enables You To
<code>-C</code>	Compare the backup file with the source file.
<code>-i</code>	Run the <code>restore</code> command in restore mode to restore back-ups partially.
<code>-r</code>	Perform a complete recovery of the backed up files.
<code>-f {/location of the backup file}</code>	Specify the location of the backup file.

Volume Number

While making backups of large files on removable storage devices, such as tape drives, the total size of the files will be split into smaller volumes and stored in multiple tape drives with each tape drive identified with a specific volume number. When you want to restore the backup made on multiple volumes, specify the volume number starting from the last volume number to the first volume number. The hard disk, because it is a single volume, will always have the volume number 1.

Restoring Files with the `tar` Command

The command `tar -xvf` will restore the entire contents of the source file or directory structure. To restore a portion of a tar file, use the path and name of the file you wish to extract. You must use the exact path and name that was used when you created the tar file. You can also make restores interactive by using the command `tar -wxvf [destination] [source]`.

Restoring Files with the `cpio` Command

The main reason you need to back up data is so that you can retrieve the data if the file gets corrupted or deleted. If you use the `cpio` command to move files to another location, you will need to get the files out of the archive file so that you can use them. The format of the copy-in option is `cpio -icdv < [archive_file name]`.

How to Back Up and Restore Files

Procedure Reference: Archive Using the `dump` Command

To archive using the `dump` command:

1. Log in as root in the CLI.
2. To make a complete backup, enter `dump -0 -f {target file} {source file}`.
3. To add updates to the existing backup file, enter `dump -{Hanoi Sequence} -f {target file} {source file}`.

Procedure Reference: Back Up Files Using the `tar` and `gzip` Commands

To back up files using the `tar` and `gzip` commands:

1. Determine the files you want to back up and put them in a directory.
2. Group all the files using the `tar` command.

3. Compress the tar file using the `gzip` command.
4. Save the file in another location (FTP site, CD, DVD, tape, floppy disk, and so on).

Procedure Reference: Restore Backups Using the `restore` Command

To restore backups using the `restore` command:

1. Log in as root in the CLI.
2. Navigate to the directory where you want to restore backed up files.
3. Restore backups.
 - To restore a backup taken using the `dump` command, enter `restore -rf /{location of the backup file}`.

Procedure Reference: Restore Files from a Backup Using the `gzip` and `tar` Commands

To restore files from a backup using the `tar` and `gzip` commands:

1. Copy the files from your backup location (FTP site, CD, DVD, tape, floppy disk, and so on).
2. Unzip the files using the `gzip` command.
3. Untar the files using the `tar` command.
4. If needed, move the individual saved files back to their respective locations.

ACTIVITY 4-9

Performing Backups

Before You Begin:

1. You have logged in as root in the CLI.
2. To create the Reports directory in the root directory, enter `mkdir Reports`.
3. To navigate to the `/root/Reports` directory, enter `cd Reports`.
4. To create the project file to store the project data, enter `vi project`.
5. Save and close the file.
6. To clear the terminal screen, enter `clear`.

Scenario:

Your colleague, Chris, is working on a very important project, and he wants to make a daily backup of his system. He also wants a reminder to be set to create backups whenever he logs in to his system.

All project-related files are in the `/root` directory and they need to be saved as `project_backup` in the `/tmp` directory.

What You Do	How You Do It
1. Make a backup of the /root files in the /tmp directory.	<ol style="list-style-type: none"> To make a complete backup, enter <code>dump -0 -f /tmp/project_backup /root</code> Observe that the message "DUMP : DUMP IS DONE" is displayed in the last line indicating that the backup was successful. To clear the terminal screen, enter <code>clear</code> To compress the backup file, enter <code>bzip2 /tmp/project_backup</code>
2. Set a reminder during system login to perform backups.	<ol style="list-style-type: none"> Enter <code>vi /etc/issue</code> To navigate to the end of the file, press Shift+G. To shift to a new line, press O. Type <i>Welcome to Linux! Remember to Backup Your Project Data</i> Press Esc. Save and close the file.
3. Verify that the reminder is displayed when the user logs in the next time.	<ol style="list-style-type: none"> To verify that the reminder is displayed in the login screen, enter <code>logout</code> Observe that the message "Welcome to Linux! Remember to Backup Your Project Data" is displayed. Log in as the root user.

ACTIVITY 4-10


Restoring Backed up Data

Before You Begin:

- 1. You are logged in as root in the CLI.
- 2. Open the /etc/issue file in the vi text editor and remove the last line that reminds the user to backup project data. Save the file and close the editor.
- 3. Log out of the CLI. Log in as root in the CLI.
- 4. Enter `rm -rf /root/Reports`.
- 5. To clear the terminal screen, enter `clear`.

Scenario:

You observe that some of your project files are missing from the Reports directory. Because you make a daily backup of your work, you decide to restore the missing files from the backup. The backup file is available in the /tmp/project_backup.bz2 location.

What You Do	How You Do It
<div>1. Identify the missing directory and files.</div> <div> Step 1a may take a few minutes.</div>	<div>a. To decompress the file, enter <code>bunzip2 /tmp/project_backup.bz2</code></div> <div>b. To view the missing directory and files, enter <code>restore -C -f /tmp/project_backup</code></div> <div>c. To clear the terminal screen, enter <code>clear</code></div>

2. Switch to the restore mode.
 - a. Enter `cd /`
 - b. To switch to restore mode, enter `restore -i -f /tmp/project_backup`
 - c. At the restore prompt, enter `cd root`

3. Extract missing files.
 - a. To add the directory that needs to be restored, enter `add Reports/`
 - b. To extract the directory from the backup file, enter `extract`
 - c. To specify the volume number, enter `1`
 - d. To accept the default owner or mode of the files to be extracted, enter `y`
 - e. To quit restore mode, enter `quit`
 - f. To check if the Reports directory has been restored, enter `ls /root/Reports`
 - g. Observe that the project file has been restored. To clear the terminal screen, enter `clear`
 - h. Enter `logout`

TOPIC G

Manage Databases Using MySQL

Previously, you worked with files in a Linux filesystem. In addition to storing data in text files, you may need to store data in a format that will allow you to easily retrieve it when required; a database will serve this purpose. In this topic, you will work with MySQL.

A text file can store volumes of data, but retrieving it will be a problem because you may have to manually locate the information you are looking for. Databases, such as MySQL, allow you to store data in an organized manner, which enables efficient retrieval of specific data. This will save you time and effort.

Databases

Definition:

A *database* is an organized collection of information. It is used to facilitate easy storage and retrieval of data. In a database, data may be grouped into a series of records, which can be further organized into smaller segments of data called *fields*. A table is the basic storage unit of a database and it consists of rows and columns. The model of a database decides the way data is organized in it.

Example:

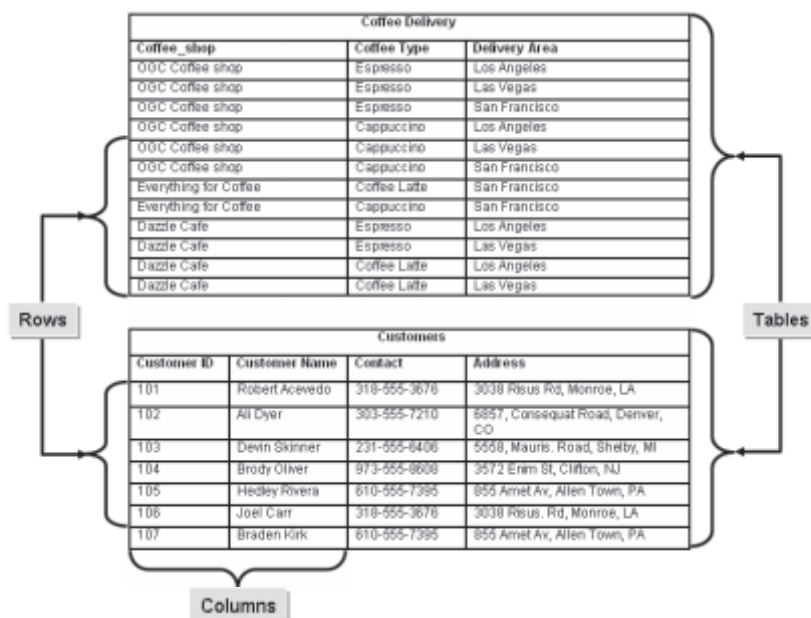


Figure 4-22: A database consisting of two tables.

Relational Databases

A *relational database* stores logically related data consistently in the form of related tables. These tables are linked through common fields or columns. The data stored is independent of files and is managed by a central database engine that processes queries and manipulates data. Every row of data contains an identification key that identifies data uniquely and helps in reducing redundancy.

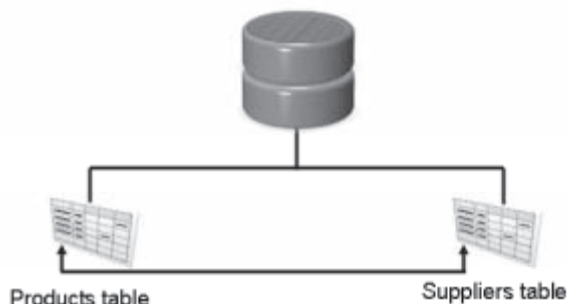


Figure 4-23: An example of a relational database.

Flat File Database

A flat file database stores data as flat files, which are static plain text documents. Flat files contain data that is structurally unrelated. The data in flat file databases cannot be retrieved or modified easily.

MySQL

MySQL is an open source *Relational Database Management System (RDBMS)* used for managing data. It is developed and distributed by Sun Microsystems. It enables you to store, retrieve, manage, organize, and share data optimally. Using *MySQL*, you can store data in one form and view it in various forms by analyzing and extracting only the relevant data from the database. *MySQL* also enables a group of networked computers to work together to enhance flexibility, efficiency, performance, scalability, and availability of the database, by eliminating time-consuming, error-prone tasks.

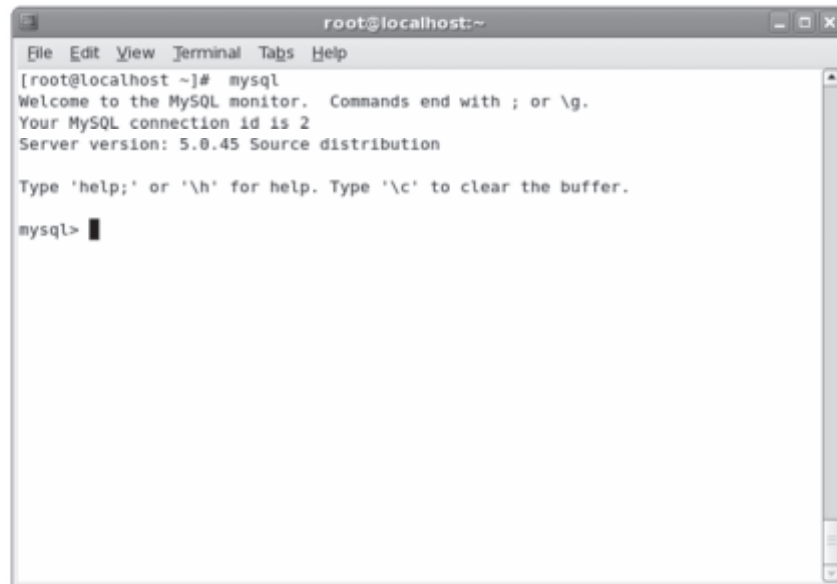


Figure 4-24: The welcome screen of the MySQL client interface.

The MySQL Configuration File

The main configuration file of MySQL, my.cnf, is located in the /etc/ directory. You can set the global options for the MySQL application in this file. The default options are usually sufficient; however, if you need to integrate MySQL with other applications, you may need to modify this file. This file allows you to set simple options, such as path to data directory; user name; and log file directory, as well as advanced options, such as table_cache and key_buffer, which can be set for the MySQL daemon.

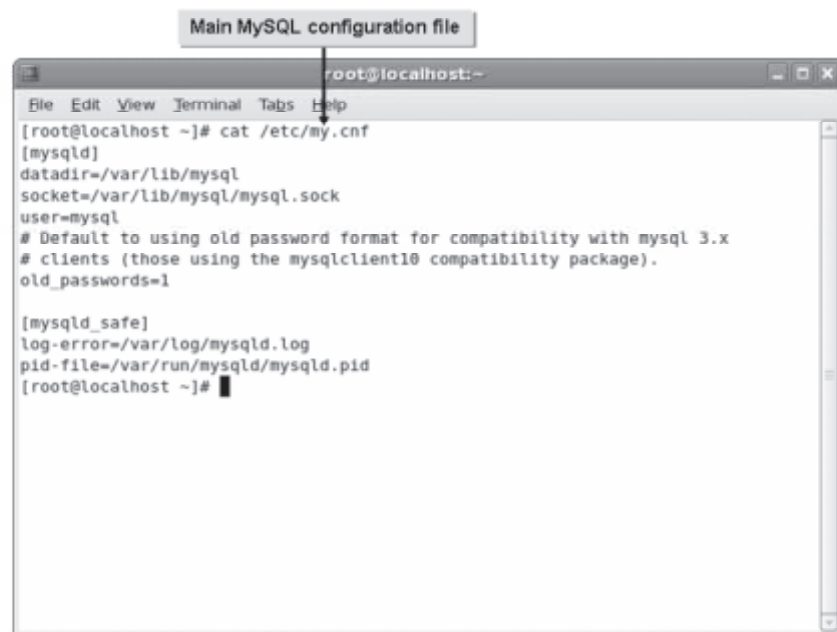


Figure 4-25: The contents of the mysql configuration file.

mysqld

The *mysqld* or MySQL daemon is also the MySQL server. It allows you to manage the MySQL server service. After installing MySQL, you need to manually start this daemon. You can start, stop, restart, or view the status of the MySQL server. This service needs to be running for clients to connect to and use MySQL.



Figure 4-26: Starting the *mysqld* service.

MySQL Commands

Clients use MySQL commands to interact with the MySQL server.

MySQL Command	Allows You To
select	Retrieve all records or records that match specific criteria.
create	Create objects, such as a database, a table, or indexes, inside an RDBMS.
alter	Modify the existing table or database.
update	Update the values in a table.
use	Make a particular database as the current database so that you can modify the objects of that database.
show	Display the tables that are available in the current database.
insert	Enter values into a row or record of the table.
describe	Display the structure of the table.
delete	Delete a row or rows from the table.

LESSON 4



The insert, update, and delete commands are also referred to as data manipulation commands because they allow you to modify the data in the table.



These commands when given with their full syntax are also referred to as statements.

Optional Clauses in the select Statement

Optional clauses can be used with the `select` statement. These clauses must be used in the order of precedence, and each of these clauses has a specific purpose.

Optional Clause	Purpose
<code>where</code>	A condition used to specify that only certain rows can be retrieved from a table.
<code>group by</code>	A column identifier used to organize data into groups.
<code>having</code>	A condition that works in conjunction with <code>GROUP BY</code> , specifying the groups to be included in the results.
<code>order by</code>	A condition that sorts query results by one or more columns.

Common SQL Queries and Actions

SQL queries can be used to perform various actions in a database. The following table illustrates various actions and their corresponding SQL queries.

Action	SQL Query
Extract all fields from a table.	<code>select * from table_name;</code>
Extract some fields from a table.	<code>select field_name_1, field_name_2,..., field_name_n from table_name;</code>
Extract all rows from a field.	<code>select field_name from table_name;</code>
Extract a row based on some condition.	<code>select field_name from table_name where condition;</code>

Range Operators Used with the select Command

The table below provides you with a list of range operators used with the `where` clause of the `select` command.

Condition	Use	Example
<code>in</code>	Determines if a certain value is equal to any value in a specific list of values.	<code>select * from emp where dept_id in (10,20,30);</code>

Condition	Use	Example
any, some	Compares a certain value to a specific list of values. Must be combined with one of the simple comparison operators.	<pre>select * from emp where dept_id= any (select dept_id from dept where dept_name='Sales' or dept_name='Systems');</pre>
all	Compares a value to every value in a list. Must be combined with one of the simple comparison operators.	<pre>select * from emp where salary >= all (select avg(basic) from emp group by dept_id);</pre>
between a and b	Determines if a value is greater than or equal to a but less than or equal to b.	<pre>select * from emp where dept_id between 10 and 50;</pre>

Joins

Definition:

A *join* is a query that is used to combine values in two or more tables in a relational database. It results in a temporary table called the joined table. A join connects tables by using their key fields.

Example: Join Two Tables

You have two tables Employees and Projects. The Employees table has the EmployeeName and ProjectID fields, and the Projects table has the ProjectID and ProjectName fields. All the ProjectIDs appearing in the Employees table are not listed in the Projects table and all the ProjectIDs appearing in the Projects table are not listed in the Employees table. To analyze which of the employees are assigned to a project and which of the projects have no employees assigned, you need to combine the information contained in these tables by using the join query.

Types of Joins

Joins are broadly classified into two categories, inner joins and outer joins.

Join Type	Description
Inner join	Allows only matching records to exist in the result set of the two joined tables.
Outer join	Selects all the values from one table and only those values from the second table that have matching values in the joined field.

How to Manage a Database Using MySQL

Procedure Reference: Install MySQL

To install MySQL:

1. Log in as root in the GUI.
2. Insert the required CD in the drive.
3. In the File Browser window, select the MySQL files and click install.
4. If necessary, select the additional files and restart the installation.
5. Verify that the installation was successful by viewing the message displayed.

Procedure Reference: Start the MySQL Daemon Service and Set it to Run Automatically

To start the MySQL daemon service and set it to run automatically:

1. To start the mysqld service, on the terminal, enter `service mysqld start`.
2. To automatically start the mysqld service at the system startup, enter `chkconfig mysqld on`.
3. If necessary, to view the status of the mysqld service, enter `service mysqld status`. To stop the MySQL server or restart the server, you can use the `service mysqld stop` and `service mysqld restart` commands, respectively.

Procedure Reference: Locate the MySQL Configuration File

To locate the MySQL configuration file:

1. If necessary, to update the locate database, enter the `update` command.
2. Change to the `/` directory.
3. To locate the path of the MySQL configuration file, enter `locate my.cnf`.
4. If necessary, open the `my.cnf` file in any text editor and modify the settings in the `my.cnf` file. To apply the changes, restart the server.

Procedure Reference: Use MySQL Commands

To use MySQL commands:

1. To connect to the MySQL server, type `mysql`.
2. To use the MySQL commands, at the **mysql** prompt, enter the required commands in the format `{commands};`.
3. To exit from the **mysql** prompt, type `quit`.

Procedure Reference: Execute an Existing sql Script

To execute an existing sql script:

1. Log in as root.
2. Copy the `{filename}.sql` file to the `/var/lib/mysql` directory.
3. To connect to the MySQL server, type `mysql`.

4. To make it the current database, at the **mysql** prompt, type `use {database name};`.
5. To execute the sql commands, type `source {file name}.sql;`.
6. If necessary, to verify that the script was successfully executed, type suitable sql commands.

Procedure Reference: Add Rows to a Table

To add rows to a table:

1. To display a description of the table, enter `desc {table name};`.
2. Identify the values for fields that need to be added in the table.
3. To insert a row of data, enter `insert into {table name }({first field name},[second field name],..., [last field name]) Values ({first field value},[second field value]...,[last field value]);`.

Procedure Reference: Modify Data

To modify data:

1. To display a description of a table, enter `desc {table_name};`.
2. To modify data in the specified fields, enter `update {table_name} set {first_field} = [value1], {second_field} = [value2] where {condition};`.
3. Enter the appropriate command to delete data from the table.
 - To delete a row based on the specified condition, enter `delete FROM {table_name} where {condition};`.
 - To delete all the rows of a table, enter `delete from {table_name};`.

ACTIVITY 4-11

Working with MySQL

Before You Begin:

- 1. Switch to the GUI.
- 2. Navigate to the /rhelsource/Server folder.

Scenario:

A junior database administrator joined your organization. As a Linux administrator, you are required to help the junior administrator install a web-based database on the Linux system. In addition, you need to ensure that clients are able to connect to the database.

What You Do	How You Do It
1. Select MySQL files.	<ul style="list-style-type: none">a. To navigate to MySQL packages, in the Server - File Browser window, type mb. Observe that a text box is displayed at the bottom-right of the window. In the text box, type yc. Observe that the mysql-5.0.45-7.el5.i386.rpm file is automatically selected.d. To view the other files, press Page Down.e. To select the file, press Ctrl and click mysql-server-5.0.45-7.el5.i386.rpm.
2. Select the other files.	<ul style="list-style-type: none">a. Scroll down till you locate the perl-DBD package.b. To select the file, press Ctrl and click perl-DBD-MySQL-3.0007-2.el5.i386.rpm.c. To select the file, press Ctrl and click perl-DBI-1.52-2.el5.i386.rpm.d. Verify that the status bar displays the message "4 items selected (14.6 MB)."

3. Install MySQL packages.
 - a. Right-click any of the selected packages and choose the **Open with "Software Installer"** option.
 - b. In the Installing packages window, observe that four packages are listed.
 - c. Click **Apply**.
 - d. In the **Software installed successfully** message box, click **OK**.
 - e. Close the Server - File Browser window.

 4. Start the MySQL daemon and verify that the installation was successful.
 - a. To display the terminal window, choose **Applications→Accessories→Terminal**.
 - b. To start the MySQL daemon, enter **service mysqld start**
 - c. Observe that the **OK** status message is displayed after the "Starting MySQL" message, indicating that the MySQL daemon was successfully started.
 - d. To automatically start the MySQL daemon service, enter **chkconfig mysqld on**
 - e. To verify that you can connect to the MySQL server, enter **mysql**
 - f. Observe that the **mysql** prompt is displayed indicating that MySQL is functional and you can use it to create databases.
 - g. To exit the **mysql** prompt, enter **quit**
 - h. To clear the terminal window, enter **clear**
-
-

ACTIVITY 4-12

Executing Commands from Existing sql Script

Data Files:

- users.sql

Before You Begin:

1. Switch to the CLI.
2. Log in as root.
3. To change to the Managing_Files directory, enter
cd /085099Data/Managing_Files.
4. To clear the terminal screen, enter clear.

Scenario:

The database administrator has some sql scripts that need to be reused in Linux. You need to help the database administrator execute a sample script in Linux to populate a new database and update data as required.

Updates required to be made are:

1. New record to be added for eric with userid 503.
2. User name of userid 508 to be changed to “pat” from “Pat.”
3. Record with userid 509 to be deleted.

What You Do	How You Do It
1. Copy the users.sql file in the correct location and connect to MySQL.	<div>a. To copy the script file to the mysql directory, on the terminal, enter cp users.sql /var/lib/mysql</div> <div>b. To change to the mysql directory, enter cd /var/lib/mysql</div> <div>c. To connect to the MySQL server, enter mysql</div>
2. Create a new userinfo database and make it the current database.	<div>a. To create a new database, at the mysql prompt, enter create database userinfo;</div> <div>b. To make it the current database, enter use userinfo;</div> <div>c. Observe that the message “Database changed” is displayed.</div>

3. Execute the `users` script and verify the values.
 - a. To execute the script, enter **`source users.sql;`**
 - b. Observe that the message "Query OK" is displayed because the script is executed.
 - c. To view the existing tables, enter **`show tables;`**
 - d. To view all records in the `users` table, enter **`select * from users;`**

 4. Modify the records of the database based on the requirement.
 - a. To add a new record for Eric, enter **`insert into users values ('503', 'eric');`**
 - b. To verify that the new record is inserted, enter **`select * from users;`**
 - c. To update the user name, enter **`update users set user_name='pat' where user_id='508';`**
 - d. To verify that the record is updated, enter **`select * from users;`**
 - e. To delete the record, enter **`delete from users where user_id='509';`**
 - f. To verify that the record is deleted, enter **`select * from users;`**
 - g. To sort the output based on the `user_id` field, enter **`select * from users order by user_id;`**
 - h. Observe that the sorted records are displayed on the screen.
 - i. To exit the `mysql` prompt, enter **`quit`**
 - j. To clear the terminal screen, enter **`clear`**
-
-

Lesson 4 Follow-up

In this lesson, you located files, linked related files, created and edited files using a text editor, backed up and restored files, and explored MySQL. This will help you customize the Linux system to your needs.

1. How can you perform a comprehensive search on your system?
2. Which text editor in Linux do you prefer? Why?

LESSON 5

Working with Linux Permissions and Ownership

Lesson Time

1 hour(s), 15 minutes

In this lesson, you will work with Linux permissions and ownership.

You will:

- Modify permissions on files and directories.
- Modify default permissions applied to files and directories.
- Modify ownership of files and directories.
- Set advanced permissions.

Introduction

While working with Linux files, you may need to modify the permissions and ownership of these files. In this lesson, you will work with Linux permissions and ownership.

In Linux, changing permissions and ownership of files will enable you to restrict or assign those files to certain users. This will increase the overall security of your system. Novice users with high privileges can cause serious damage to a Linux system.

This lesson covers all or part of the following CompTIA Linux+ Powered by LPI certification objectives:

- Topic A:
 - Objective 104.5
- Topic B:
 - Objective 104.5
- Topic C:
 - Objective 104.5
- Topic D:
 - Objective 104.5, Objective 110.1

TOPIC A

Modify File and Directory Permissions

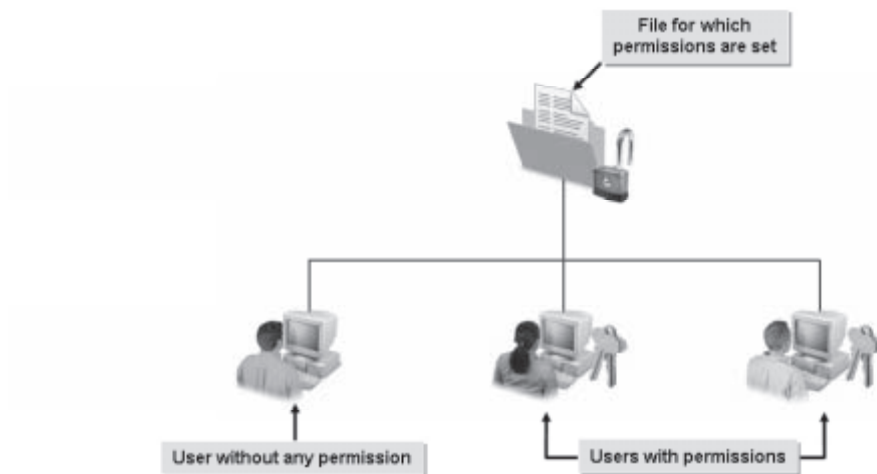
Now that you can work with Linux files, you can begin to alter their permissions to restrict who can access or edit various files. In this topic, you will modify file and directory permissions.

Systems in your workplace may hold files and other data that should not be made accessible to all users. To prevent accidental modification or deletion of important information, certain files should be accessible only to the root user or to the owner of the file. As a system administrator, it is your responsibility to modify file and directory permissions that will enable you to restrict or allow user access to system critical and generic files.

Permissions

Definition:

Permissions are access rights assigned to users, which enable them to access or modify files and directories. Permissions can be set at different levels and for different access categories. The `ls -l` command can be used to view the permissions of a file.

Example:**Figure 5-1:** *Permissions set for a few users.*

The `ls -l` command gives you a long list of the files and directories in your current working directory. Each item in the list consists of 15 columns.

The contents of the columns are described in the following table.

Column Number	Description
0	The first column (known as column 0) indicates whether it is a file (-) or a directory (d).
1-3	User (owner) permissions. The user for whom these permissions are valid is listed in column 11.
4-6	Group permissions. The group for whom these permissions are valid is listed in column 12.
7-9	Other users' permissions. Any other user, besides the specified user and group, receives these permissions.
10	Number of links. Files generally have a link count of 1. For directories, the link count is the number of directories under it plus two; one for the directory itself and one for the parent. Links are similar to Windows shortcuts; they point to the location where the file exists and allow you to access and view the file.
11	Displays the owner of the file or directory.
12	Displays the group to which the owner of the file belongs. All members of this group have the permission listed in columns 4-6. The administrator adds users to a group so that permissions can be assigned to the group rather than to each user.
13	Lists the size (in bytes) of the file or directory.
14	Displays the date and time the file was created or last modified.
15	Displays the file or directory name.



Use the `ls -ld [directory name]` command to list directory entries of the specified directory. The contents of the directory will not be displayed.

Access Categories

Access categories in Linux permissions decide how Linux interprets the permissions of a file. If a user's UID matches the permissions of the file, the user level permissions are applied. If the GID of the user matches the permissions, group permissions are granted. If neither of the permissions match, the general permissions for others are applied. The symbols for the access categories are listed in the following table.

Access Category	Description
u	Modifies permissions at user level.
g	Modifies permissions at group level.
o	Modifies permissions for other users.
a	Modifies permissions for all users globally.

Permission String

The output of the `ls -l` command shows the permission string for a file or directory. The permission string contains ten characters. The first character indicates the type of file; *d* for directory and hyphen (-) for file. Characters at the second, third, and fourth positions denote permissions of the owner or user of the file or directory. Characters at the fifth, sixth, and seventh positions denote group permissions, and the characters at the eight, ninth, and tenth positions denote permissions for others.

Permission Levels

Permissions are granted or denied by the owner of the file. The following table lists the levels of various permissions and their description.

Level of Permission	Description
User level r/w/x permission	Only the owner can read, write, and execute the file.
Group level r/w/x permission	Only the members of groups to which the owner belongs to can read, write, and execute the file.
Other level r/w/x permission	All users can read, write, and execute the file.

File Owner

A *file owner* is the user who creates a file or directory. The file owner can set permissions to specify whether other users or groups have rights to read, write, or execute the file.

The chmod Command

The `chmod` command enables you to modify default permissions of a file or directory. Only the owner of the file or the system administrator can change the permissions of the file or directory.

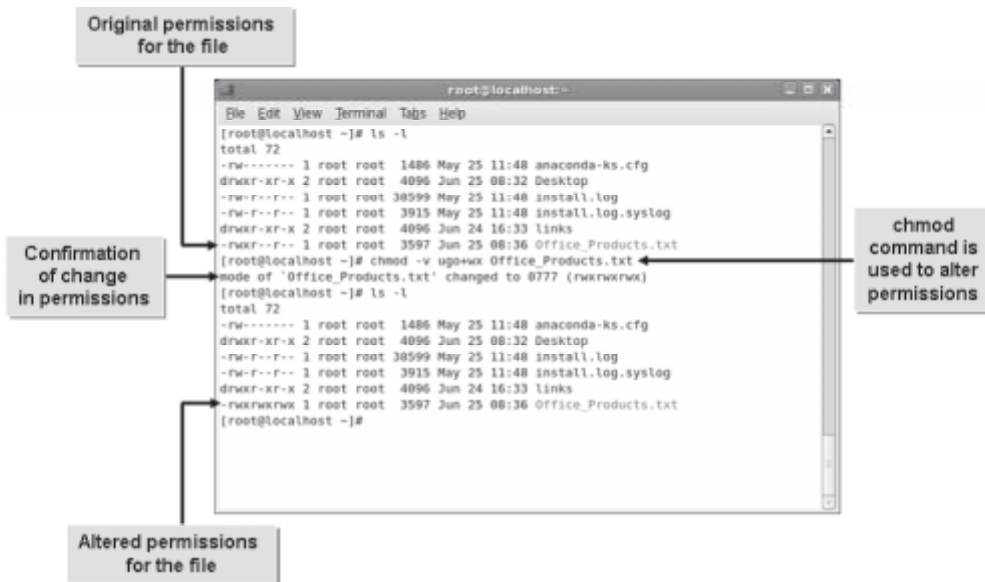


Figure 5-2: Modifying permissions using the `chmod` command.

Syntax

The syntax of the `chmod` command is `chmod [options] {mode} {file name}`.

chmod Command Options

The `chmod` command supports different options to modify permissions. One or more of these options may be used at a time.

Option	Description
<code>-c</code>	Reports changes that are made in permissions.
<code>-f</code>	Hides most error messages.
<code>-v</code>	Displays a diagnostic entry for every file processed.
<code>-R</code>	Modifies permissions of files and directories recursively.

chmod Modes

The `chmod` command supports two modes: the character mode and the numeric mode. The character mode allows you to set permissions using three components, namely, access categories such as `u/g/o/a`; operators such as `+/-/`; and permission attributes such as `r/w/x`. The numeric mode is represented by three-digit numbers.

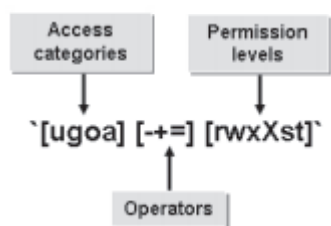


Figure 5-3: Components of the character mode.

Operators Associated with Permissions

Operators decide whether a permission is to be granted or removed. Common operators associated with Linux permissions are listed in the table below.

Operator	Description
+	Grants permissions.
-	Denies permissions.
=	Causes the permissions assigned to overwrite other existing permissions. Assigns permissions similar to those of the reference file.

Permission Attributes

Permission attributes define exactly what a user is allowed to do with a particular file. The three permission attributes are listed in the table.

Permission Attribute	Allows You To
r (read)	View file content.
w (write)	Modify file content.
x (execute)	Run a file (if it is an executable program and is combined with the read attribute).

Changing Permissions Using the Character Method

The permissions of a file or directory can be changed using the character method. The syntax of the `chmod` command when using this method is `chmod [options] {access categories}{operators}{permission levels} {file name or directory name}`.

Changing Permissions Using Octal Permission Numbers

Linux systems use octal (base-8) numbers to specify permissions. Each permission (r, w, and x) has an associated number.

Octal Number	Attribute	Letter
4	read	r

Octal Number	Attribute	Letter
2	write	w
1	execute	x

By adding the octal numbers for the permissions you want to grant, you get the overall permission number to assign to a directory or file. Full permissions (read, write, and execute) are equivalent to $4 + 2 + 1$, or 7. Read and write permissions are equivalent to $4 + 2$, or 6. Complete permissions are expressed as a three-digit number, where each digit corresponds to the user, the group, and other permissions, respectively.

The syntax of the number method to change permissions is `chmod {number} {file name}`.

How to Modify File and Directory Permissions

Procedure Reference: View File or Directory Permissions

To view file or directory permissions:

1. Log in as a user.
2. View the permissions of a file or directory.
 - View the permissions of a file or directory, as necessary, from the command line.
 - To view the permissions of a file, enter `ls -l {file name}`.
 - To view the permissions of a directory, enter `ls -ld {directory name}`.
 - View the permissions of a file or folder using the Nautilus browser.
 1. Right-click the file or folder and choose **Properties**.
 2. To view the permissions of the file or folder, select the **Permissions** tab.

Procedure Reference: Modify File or Directory Permissions

To modify file or directory permissions:

1. Log in as root.
2. Change the permissions of a file or directory in the CLI or the GUI.
 - To modify permissions in the CLI, enter `chmod [options] {file or directory name}`.
 - Or, modify permissions in the GUI.
 1. Right-click the file or directory and choose **Properties**.
 2. Select the **Permissions** tab.
 3. From the **File Access** or **Folder Access** drop-down list, select the desired permission for owner, owner groups, and other groups.

ACTIVITY 5-1

Modifying File and Directory Permissions Using the Command Line

Data Files:

- Training_Policy.txt

Before You Begin:

1. You have logged in as root in the CLI.
2. To change to the root directory, enter `cd /root`.
3. To copy files, enter `cp -p /085099Data/Linux_Permissions/* /root`.
4. To change the file permissions, enter `chmod 700 Training_Policy.txt`.
5. To clear the terminal screen, enter `clear`.

Scenario:

A new employee training policy is to be implemented in your organization and your HR manager wants all the employees to be able to read the newly created Training_policy.txt policy document. You have been given the task of assigning permissions to all users so that they can read the file.

What You Do	How You Do It
1. View the permissions of the Training_Policy.txt document.	<div>a. To view the permissions of the Training_Policy.txt file, enter <code>ls -l</code></div> <div>b. Observe that the root user has read, write, and execute permissions on the Training_Policy.txt file, while the group and others do not have any permissions.</div>

2. Modify the permissions using the character method and verify the change.
 - a. To modify the permissions using character mode, enter `chmod -v go=r Training_Policy.txt`
 - b. Observe that the message "mode of Training_Policy.txt changed to 0744 (rwxr--r--)" is displayed, indicating that the group and others have now been granted read permission to the file.
 - c. To view the new permissions of the Training_Policy.txt file, enter `ls -l`
 - d. Observe that the permissions of the file have been modified to allow all users to read the file.
 - e. To clear the terminal screen, enter `clear`
-

ACTIVITY 5-2

Modifying File and Directory Permissions Using the Nautilus Browser

Data Files:

- Skill_Certification_Policy.txt

Before You Begin:

1. You have logged in as root in both the CLI and the GUI.
2. Switch to the GUI.
3. Display the terminal window.
4. To change to the root directory, on the terminal window, enter `cd /root`.
5. To change the file ownership, enter `chown jsmith Skill_Certification_Policy.txt`.
6. To add a group named Human_Resources, enter `groupadd Human_Resources`.
7. To change group ownership of the Skill_Certification_Policy.txt file to the Human_Resources group, enter `chgrp Human_Resources Skill_Certification_Policy.txt`.
8. To assign file permissions, enter `chmod 600 Skill_Certification_Policy.txt`.
9. Close the terminal window.

Scenario:
The HR manager, Rachel, updated the company policy document Skill_Certification_Policy.txt on skill certification and wants you to make this policy document accessible to all employees. You want to show her how to modify the permissions of files and directories using the Nautilus browser because she is familiar only with the GUI.

What You Do	How You Do It
1. View the permissions of the Skill_Certification_Policy.txt file.	<div>a. To view the files and folders, on the desk-top, double-click root's Home.</div> <div>b. In the root - File Browser window, right-click the Skill_Certification_Policy.txt file and choose Properties.</div> <div>c. To view the permissions of the file, in the Skill_Certification_Policy.txt Properties dialog box, select the Permissions tab.</div> <div>d. On the Permissions tab, observe that jsmith is the owner of the file and has read and write access to the file. In addition, the group Human_Resources does not have any access to the file.</div>
2. Modify the permissions of the Skill_Certification_Policy.txt file using the Properties dialog box.	<div>a. From the Access drop-down list, which is below the Group drop-down list, select Read-only.</div> <div>b. From the Access drop-down list, which is below the Others drop-down list, select Read-only.</div> <div>c. Click Close to save the modifications and exit the Skill_Certification_Policy.txt Properties dialog box.</div> <div>d. Close the root - File Browser window.</div>

TOPIC B

Modify Default Permissions

Previously, you modified file and directory permissions. Now, you need to know how to alter default permissions of files. In this topic, you will modify default permissions in Linux.

Modifying default file permissions will allow you to set higher or lower security levels for files created by users. This will allow high-level users to create files that are completely secure from other users.

Default File and Directory Permissions

In Linux, default permissions are assigned to newly created files and directories based on user privileges. For files created by the root user, the default permission is 644, which means that the root user has read and write permissions, while group users and others will have only read permission. For directories created by the root user, the default permission is 755, which means that the root user has read, write, and execute permissions, while group users and others will have only read and execute permissions. In the case of users with limited access rights, Linux assigns a permission of 664 for newly created files and 775 for newly created directories. These default permissions are determined by the user file creation mask, or umask. However, the default permissions may be altered by the root user.

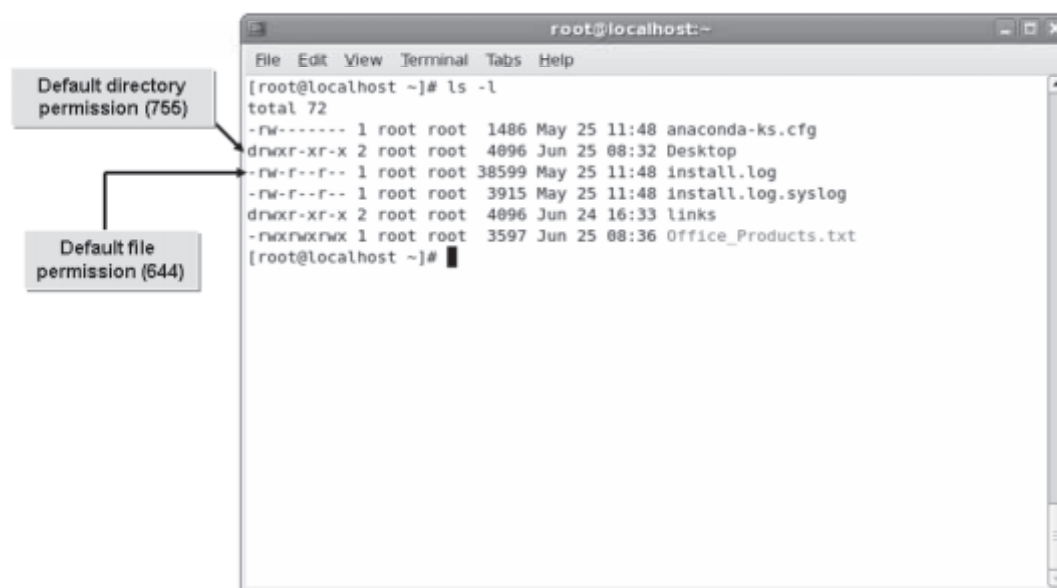


Figure 5-4: The `ls` command displaying the default file and directory permissions.

The umask Command

The `umask` command automatically alters the default permissions on newly created files and directories. The default permissions on newly created files and directories can be changed for security reasons.

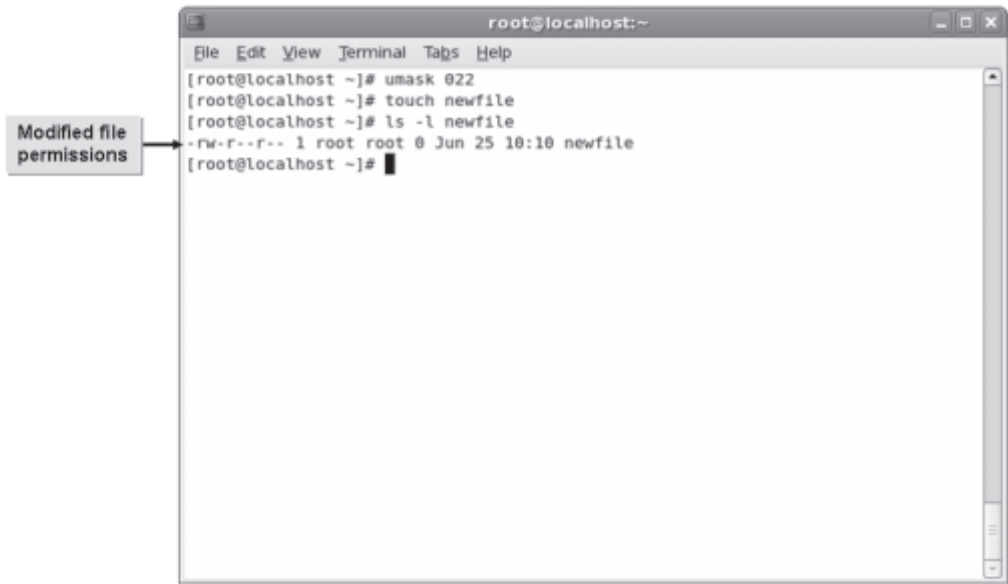


Figure 5-5: Default file permissions modified using the umask command.

Syntax

The syntax of the *umask* command is *umask {number}*.

The Effect of umask on Files

By default, the base permissions for nonexecutable files in Linux are *rw-rw-rw-* or 666. By entering *umask 0022*, the permissions assigned to all files, created from that moment until the system is restarted, will be *rw-r--r--* (644). The numbers given with the *umask* command specify the permissions that need to be cleared from the default settings. The first digit allows you protect the file by setting advanced permissions. The other three digits allow you to set the normal permissions.

Number	Clears
0	Nothing from the users' default permissions, leaving <i>rw-</i> .
2	Write permission from the group, leaving just <i>r--</i> .
2	Write permission from others, leaving just <i>r--</i> .

These settings correspond to the default umask of the root user.

The Effect of umask on Directories

By default, the base permissions for directories in Linux are *rw-rw-rw-* or 777. By entering *umask 0022*, the permissions assigned to all directories, created from that moment until the system is restarted, will be *rw-r--r--* (755). The numbers given with the *umask* command specify the permissions that need to be cleared from the default settings. The first digit allows you to protect the directory by setting advanced permissions. The other three digits allow you to set the normal permissions.

Number	Clears
0	Nothing from the users' default permissions, leaving <code>rwX</code> .
2	Write permission from the group, leaving just <code>r-X</code> .
2	Write permission from others, leaving just <code>r-X</code> .

These settings correspond to the default umask of the root user.

How to Modify Default Permissions

Procedure Reference: Modify Default Permissions

To modify default permissions:

1. Log in as root.
2. To change the default umask value, enter `umask {umask number}`.
3. Create a new file to verify that files created from now on have different default permissions.

ACTIVITY 5-3

Modifying Default Permissions

Before You Begin:

1. You have logged in as root in the GUI.
2. The user account for Chris already exists on the system.

Scenario:

Your colleague, Chris, creates large number of documentation files that are used by other users on the system. Your manager would like all files created by her, from now on, to be readable and modifiable by all users.

Account details of the user:

- User name: `chris`
- Password: `myp@$sw0rd`

LESSON 5

What You Do	How You Do It
1. Change the umask value on Chris' system to 0000.	<ol style="list-style-type: none">Switch to the fourth terminal.Log in as chris on Chris' system.To view the current umask value, enter umaskObserve that the umask value is displayed as 0002.To create a test file with existing permissions, enter touch newfile1To alter the umask value, enter umask 0000
2. Check whether the umask value has been changed.	<ol style="list-style-type: none">To view the new umask value, enter umaskObserve that the umask value is now displayed as 0000.
3. Create a file and compare its permissions to an existing file.	<ol style="list-style-type: none">To create a file, enter touch newfile2To view the permissions of the files, enter ls -l new*Observe the difference in file permissions of newfile1 and newfile2.Log out of the terminal.

TOPIC C

Modify File and Directory Ownership

With an understanding of default permissions, you can modify the owners of files and directories. A user or group may not want other users to access the files created by them. Also, users may require access to files created by other users. In this topic, you will modify file and directory ownership.

Imagine that you have been working on a project that is to be taken over by one of your colleagues. Consequently, you will need to transfer the ownership of all the files you created for this project to your colleague. Modifying file and directory ownership will enable you to help your colleague make the transition to project owner.

The `chown` Command

The `chown` command can be used to change the owner, the group, or both for a file or directory.

The following table describes how to use this command.

Command Syntax	Description
<code>chown {user name} {file name}</code>	Changes the owner but not the group.
<code>chown {user name:group name} {file name}</code>	Changes the owner and the group.
<code>chown {user name:} {file name}</code>	Changes the owner and the group. The group will be changed to the specified user's login group.
<code>chown {:group name} {file name}</code>	Changes the group but not the owner. This is the same as using the <code>chgrp</code> command.

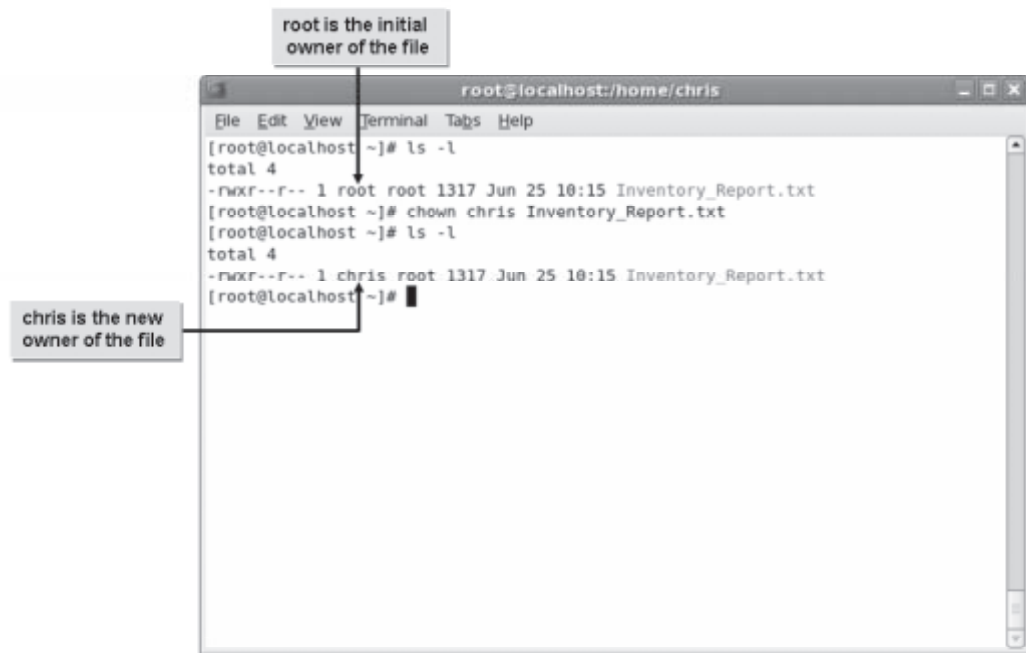


Figure 5-6: File ownership changed using the *chown* command.

Recursively Changing Ownership

You can combine the *chown* command with the *-R* option to recursively change ownership through a directory structure. You can also use metacharacters to change ownership of groups of files at the same time.

Changing Group Ownership

The *chgrp* command is used to change the group ownership of a file or directory. The syntax of the command is *chgrp {group} {file name}*.

How to Modify File and Directory Ownership

Procedure Reference: View File or Directory Ownership

To view file or directory ownership:

1. Log in as a user.
2. View the ownership of a file or directory in the desired mode.
 - View the ownership of a file or directory at the command prompt.
 - To view the ownership of a file, enter *ls -l {file name}*.
 - To view the ownership of a directory, enter *ls -ld {directory name}*.
 - View the ownership of a file or directory using the Nautilus browser.
 1. Right-click the file or directory and choose **Properties**.
 2. To view the ownership of the file or directory, select the **Permissions** tab.

Procedure Reference: Modify File or Directory Ownership

To modify file or directory ownership:

1. Log in as root.
2. Change the ownership of a file or directory.
 - Modify file or directory ownership at the command prompt.
 - To change the user ownership of the file or directory, enter `chown [command options] [username][:{group name}] {file or directory name}`.
 - To change the group ownership of the file or directory, enter `chgrp [command options] {group name} {file or directory name}`.
 - Modify file or directory ownership using the Nautilus browser.
 1. Right-click the file or directory and choose **Properties**.
 2. Select the **Permissions** tab.
 3. Make changes to the ownership as necessary.
 - From the **Owner** drop-down list, select the owner of the file or directory at user level.
 - From the **Group** drop-down list, select the owner of the file or directory at group level.

ACTIVITY 5-4

Modifying File and Directory Ownership Using the Command Line

Before You Begin:

To switch back to the first terminal, press **Ctrl+Alt+F1**.

Scenario:

Your colleague, Patrick, created a large number of files. He wants a centralized location to store them. As a system administrator, you decide to create a directory `/work_files/pat_files`, which Pat will have ownership of.

What You Do	How You Do It
1. Create the /work_files/pat_files directory and verify that it was created.	<ol style="list-style-type: none"> To switch to the /work_files directory, enter cd /work_files To create a work directory, enter mkdir pat_files To view the contents of the /work_files directory with ownership details, enter ls -l Observe that the root is the owner of the pat_files directory.
2. Change the ownership of the pat_files directory to the user, Patrick.	<ol style="list-style-type: none"> To change the ownership of the work directory, enter chown pat pat_files To view the directory contents with ownership details, enter ls -l Observe that the owner of the pat_files directory is Patrick. Clear the terminal screen.

TOPIC D

Set Advanced Permissions

Now that you have modified file and directory ownership, you can set advanced permissions for users. There may be instances when you have to use special permissions to enable users to access files or directories. In this topic, you will set advanced permissions.

While it is desirable to allow only users with root or administrative permissions to execute certain commands, sometimes other users need to be able to issue them. Setting advanced permissions will allow other users to execute and maintain system utilities so that the Linux administrator does not have to do them for each user. This will save the administrator time and effort.

Special Permissions

Special permissions are used when normal permissions become inadequate, usually in the case of processes. With special permissions, less privileged users are allowed to execute a file that can usually be run only by the root user. Set User ID (SUID), or `setuid`, is the permission that allows a user to have similar permissions as the owner of the file. Set Group ID (SGID), or `setgid`, is the permission that allows a user to have similar permissions as the group owner of the file.

The SUID and SGID Permissions

The SUID and SGID commands are powerful tools that enable users to perform tasks without problems that could arise with users having the actual permissions of that user or group. However, these can be dangerous tools too.

While changing the permissions of a file to be either SUID or SGID, the following points should be considered:

- Use the lowest permissions needed to accomplish a task. It is recommended not to give a file the same SUID or SGID as the root user. A user with fewer privileges often can be configured to perform the task.
- Watch for back doors. If the user runs a program with the SUID set to root, then the user retains root as the effective UID when the user goes through the back door. The following can be used as back doors:
 - Programs that enable you to shell out.
 - Programs with multiple entrances and exits.

The `chattr` Command

The `chattr` command is used to change the attributes of a file on a Linux filesystem.

The following table lists the description for the options used in the syntax of the `chattr` command.

Command Option	Used To
<code>-R</code>	Recursively change the attributes of directories and their contents.
<code>-V</code>	Display the output of the <code>chattr</code> command and print the program version.
<code>-v {version}</code>	Set the version number of a file.
<code>+i</code>	Mark the file as read-only.
<code>-i</code>	Remove the read-only attribute of the file.

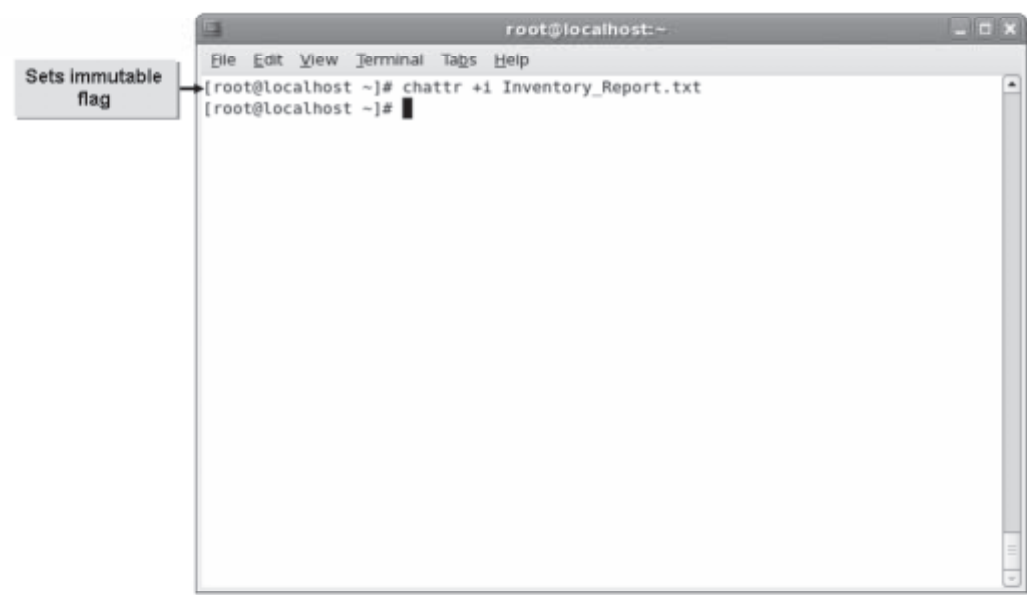


Figure 5-7: Attribute of the file set using the chattr command.

Syntax

The syntax of the `chattr` command is `chattr [-RV] [-v version] { [mode] {file names} }`.

The lsattr Command

The `lsattr` command is used to list the attributes of a file on a Linux filesystem.

The following table describes the options used in the syntax of the `lsattr` command.

Command Option	Used To
-R	Recursively list the attributes of directories and their contents.
-V	Display the program version.
-a	List all files in directories.
-d	List directories like files, instead of listing their contents.
-v	List the version number of the file.

Syntax

The syntax of the `lsattr` command is `lsattr [-RVadv] [file names]`.

Sticky Bits

A *sticky bit* is a permission bit that provides protection for files in a directory. It ensures that only the owner of a file can delete the file or directory. A sticky bit also forces a program or file to remain in memory so that it need not be reloaded when it is invoked again. A sticky bit on a file indicates to the operating system that the file will be executed frequently. Files with sticky bits are kept in the swap space or in the disk space that is set aside for virtual memory.

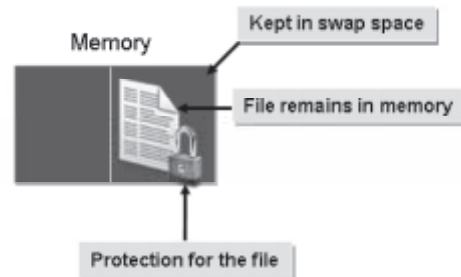


Figure 5-8: A file in the memory protected by a sticky bit.

The Immutable Flag

Definition:

The *immutable flag* is an extended attribute of a file or directory that prevents it from being modified. The immutable flag is not set on all files. It is set only on those files, such as configuration files, that should not be modified. A single directory can have a mix of mutable and immutable files and subdirectories. Also, an immutable subdirectory can have mutable files.

Example:

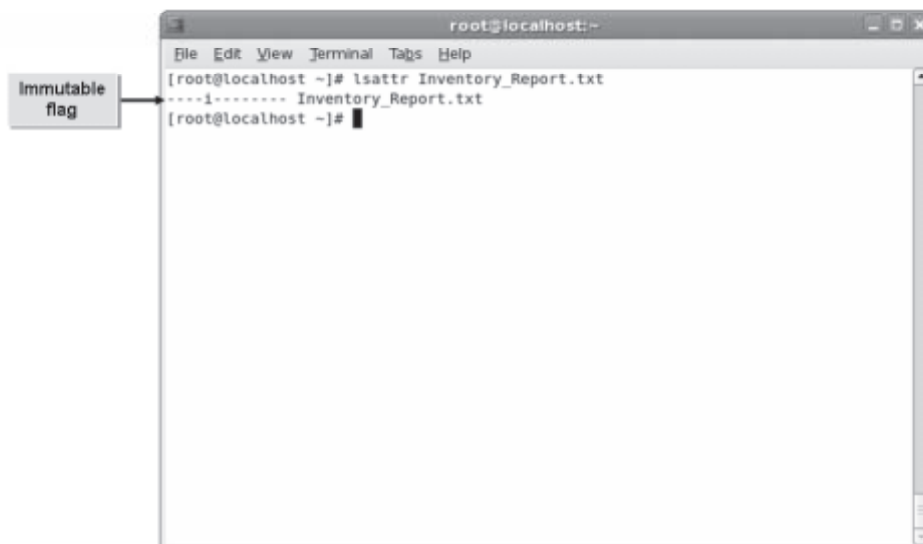


Figure 5-9: The immutable flag prevents modification of the file.

The ACL

The *Access Control List (ACL)* is a list of permissions attached to an object. Usually, a file object in Linux is associated with three sets of permissions—read, write, and execute—for the three user groups: file owner; group; and other. ACLs can be used for situations where the traditional file permission concept does not suffice. They allow the assignment of permissions to individual users or groups even if these do not correspond to the owner or the owning group.

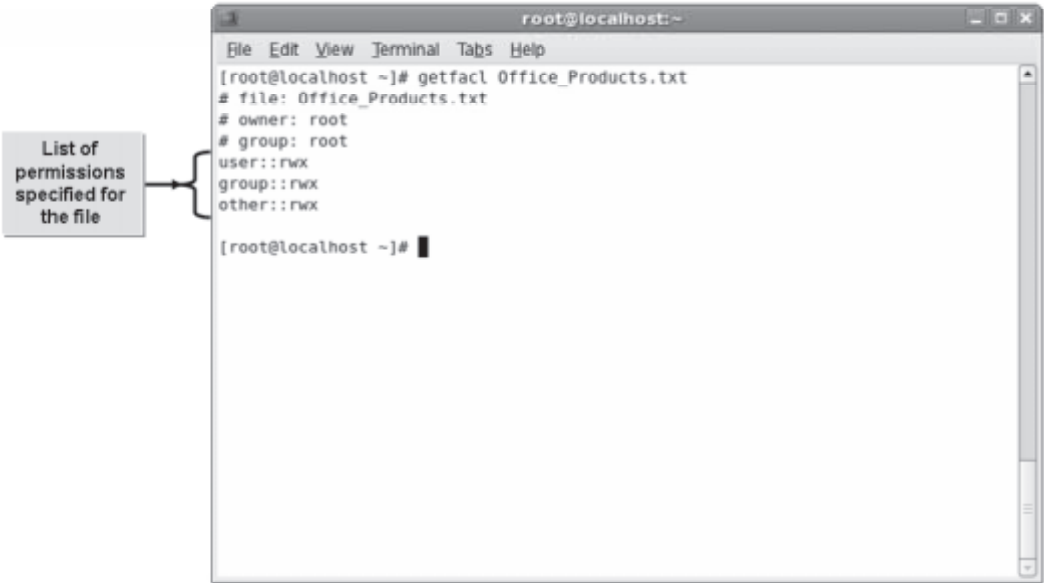


Figure 5-10: The ACL of a file displayed using the `getfacl` command.

Commands Associated with the ACL

ACLs can be managed at filesystem level or at the file and directory level. To find out the ACL specifications of a file, you can use the `getfacl` command. To set the access control specifications for files and directories, you can use the `setfacl` command with its different options.

Advanced Permission Commands

Advanced permission commands can be used effectively to set special file or directory access rights for users. Some of the common commands to set these permissions are listed in the following table along with their syntax.

Command Syntax	Used To
<code>chmod u{operator}s {file name}</code>	Set the SUID for a file.
<code>chmod g{operator}s {directory name}</code>	Set the SGID for a directory.
<code>chmod o{operator}t {file name}</code>	Set the sticky bit for a file.
<code>umask {value}</code>	Set the default file creation mode.
<code>chattr {operator}i {file name or directory name}</code>	Set the immutable flag for a file or directory.

How to Set Process Permissions

Procedure Reference: Set Special Permissions for Files and Directories

To set special permissions for files and directories:

1. Log in as a user.
2. Set special permissions for files and directories.
 - To add the SUID permission for a file, enter `chmod u+s {file name}`.
 - To add the SGID permission for a directory, enter `chmod g+s {directory name}`.
 - To add the sticky bit permission for the directory, enter `chmod +t {directory name}`.
3. If necessary, to verify the changes, enter `ls -l`.

Procedure Reference: Manage ACLs for Files and Directories

To manage ACLs for files and directories:

1. Log in as root.
2. Manage ACLs for files and directories:
 - To view the ACL for the specified file or directory, enter `getfacl {file name or directory name}`.
 - To set the ACL for the specified file or directory, enter `setfacl -m {g | u | o}:[user name or group name]:[r,w & x combination] {file name or directory name}`.
 - To inherit all the permissions for the newly created content in the specified directory name, enter `setfacl -m d:{g | u}:[user name or group name]:[r,w & x combination] {directory name}`.
 - To set the ACL for the specified file or directory, enter `setfacl -x {g | u}:[user name] {file name or directory name}`.

Procedure Reference: Change the Default Group Owner of New Files

To change the default group owner of new files:

1. Log in as root in the CLI.
2. To change the group ownership of the directory, enter `chgrp {group name} /{directory name}`.
3. If desired, to view the status of the group owner of the directory name, enter `ls -l`.
4. To set the SGID for the directory, enter `chmod g+s /{directory name}`.
5. If necessary, to view the status of the group permissions of the directory, enter `ls -l`.
6. Enter `cd /{directory name}`.
7. If necessary, enter `touch {file name}`.
8. If necessary, to verify the status of the group owner of the newly created file, enter `ls -l`.

ACTIVITY 5-5

Setting User Access to Files

Data Files:

- Salaryaccount.txt

Before You Begin:

1. You have logged in as root in the CLI.
2. To add a new user, tax, enter `useradd tax`. To change the password for the user, tax, enter `passwd tax`.
3. Type `myp$$w0rd` and press **Enter**.
4. To confirm the password, type `myp$$w0rd` and press **Enter**.
5. Create two other users by following step 2 to step 4 based on the details given below:
User name: income, Password: `myp$$w0rd`
User name: expenditure, Password: `myp$$w0rd`
6. To add the income user to the tax group, enter `usermod -G tax income`. To add the expenditure user to the tax group, enter `usermod -G tax expenditure`.
7. To log out the root user, enter `logout`.
8. Log in as tax. Type `myp$$w0rd` and press **Enter**.
9. To create a new directory, enter `mkdir Finance`. To log out the tax user, enter `logout`.
10. Log in as root. Type `p@ssw0rd` and press **Enter**.
11. To copy the data files to the Finance directory, enter `cp /085099Data/Linux_Permissions/* /home/tax/Finance`. To log out the root user, enter `logout`.

Scenario:

You are working as a junior system administrator in an organization. The finance department consists of three user groups: Income, Expenditure, and Tax. Income and Expenditure are members of the Tax group. The finance manager does not want the Tax group to be able to change the Salaryaccount.txt document located in the /home/tax/Finance directory.

User account details:

- Login name for tax user: tax
- Password for tax user: `myp$$w0rd`
- Login name for income user: income
- Password for income user: `myp$$w0rd`
- Login name for expenditure user: expenditure
- Password for expenditure user: `myp$$w0rd`

What You Do	How You Do It
1. Set the group read and execute permissions for the home directory of the tax user.	<ol style="list-style-type: none"> Log in as tax in the CLI. To switch to the home directory, enter cd .. To view the access rights of the tax directory, enter ls -l To set the group read and execute permission for the home directory of the tax user, enter chmod g+rx tax Clear the terminal screen. To view the changed access rights of the home directory of the tax user, enter ls -l
2. Remove the group write access for the Finance directory.	<ol style="list-style-type: none"> To switch to the tax directory, enter cd tax To view the access permissions of the Finance directory, enter ls -l To remove the group write permission of the Finance directory, enter chmod g-w Finance To view the changed access rights of the Finance directory, enter ls -l Log out of the account.
3. Set the read-only permission for the Finance directory.	<ol style="list-style-type: none"> Log in as root. To set the immutable flag for the Finance directory, enter chattr +i /home/tax/Finance Log out of the terminal.

LESSON 5

4. Check whether the members of the tax group are able to remove the Salaryaccount.txt file.
 - a. Log in as the **income** user.
 - b. To switch to the Finance directory, enter **cd /home/tax/Finance**
 - c. To view the contents of the directory, enter **ls**
 - d. To verify if the Salaryaccount.txt file can be deleted, enter **rm Salaryaccount.txt**
 - e. Observe that a prompt with a message to confirm the removal of a rights protected regular file is displayed.
 - f. To confirm the removal of the file, enter **y**
 - g. Observe that a message is displayed to indicate that permission is denied because the immutable flag for the directory is set.
 - h. Log out of the terminal.
-

Lesson 5 Follow-up

In this lesson, you modified permissions and ownership of files and directories in a Linux system. You also set process permissions to allow other users to execute a process generally run by an administrator, saving them both time and effort. Now, you will be able to efficiently control the security of your Linux system.

1. How can you preserve confidentiality of information on Linux systems?
2. When should default permissions be modified?

LESSON 6

Printing Files

Lesson Time
1 hour(s), 30 minutes

In this lesson, you will print files.

You will:

- Configure a local printer.
- Format text in a file and print it.
- Manage print jobs and queues.
- Configure remote printing.

Introduction

In the last lesson, you worked with files in Linux. Now, you may want to print those files containing essential information. In this lesson, you will work with printer hardware and software.

Like all standard operating systems, Linux allows its users to print files. You may have trouble viewing lengthy files continuously on a monitor and may consider printing them. Linux includes effective printing utilities that allow you to print configuration files and any other text documents you create.

This lesson covers all or part of the following CompTIA Linux+ Powered by LPI certification objectives:

- Topic A:
 - Objective 108.4
- Topic C:
 - Objective 108.4

TOPIC A

Configure a Local Printer

Previously, you worked with various files in Linux and now might want to print some of them. Before you can print a file, you must configure a printer to work with the Linux operating system. In this topic, you will configure a local printer to work with your system.

Computers at homes and offices are regularly used for printing. Like other operating systems, Linux also supports printing. However, not all printers are compatible with the Linux operating system. You must check for compatibility before selecting a printer to be used with your Linux system. Even if a printer is compatible, you will need to know how to configure it with a system before it can be used for printing.

Printer Software

Definition:

Printer software is a program that enables a printing device to print text or graphics on media. The printer software provided with a printer includes a driver and utilities. The printer driver allows users to choose settings for the printer. The printer utilities ensure that the printers are in operating condition.

Example:



Figure 6-1: *Printer software comprises drivers and utilities.*

PostScript®

PostScript® is a *Page Description Language (PDL)* that tells a printer how to display text or graphics on a page. Laser printers primarily use PostScript for printing documents. The print quality is high because it resizes fonts and images without distortion. PostScript can work on different platforms and printers, and therefore can be used to share documents on the Internet.




Figure 6-2: *PostScript helps a system communicate with a printer.*

Linux Compatible Printers

PostScript is the standard PDL supported by Linux. Therefore, most of the Linux compatible printers are postscript printers. PostScript printers support printing in Linux because PostScript Printer Definitions (PPDs) describe and provide access to printer-specific features. PPDs function as drivers for PostScript printers and provide a unified interface for the printer's capabilities.



Figure 6-3: *A PostScript printer.*

 For information about specific distributions of Linux and installation of printer drivers, visit the website of the specific distribution.

Configuring a Local Printer

When Linux is installed, you can configure a printer to work with the operating system. Using the print system manager, you can add printers to the system. A local printer is attached directly to the Linux workstation via a parallel, serial, or USB port. A remote printer is attached to a Unix or Linux machine elsewhere on the network.

 LPD (Line Printer Daemon) is a Linux system service for network printing.

 The `lpr`, `lprm`, and `lpq` commands are referred to as `lpd` legacy interfaces.

CUPS

The *Common UNIX Printing System (CUPS)* is a systematic print management system for Linux; this printing system allows a computer to function as a print server. A system running CUPS is a host that can initiate print jobs from client systems. These jobs are then processed and sent to the appropriate printer. The main advantage of CUPS is that it can process different data formats on the same print server. CUPS is designed for scheduling print jobs, processing administrative commands, and providing printer status information to local and remote programs. The CUPS configuration is accessed by using a browser window. By making changes through the browser interface, you can edit the `cupsd.conf` file, which is located in the `/etc/cups` directory.

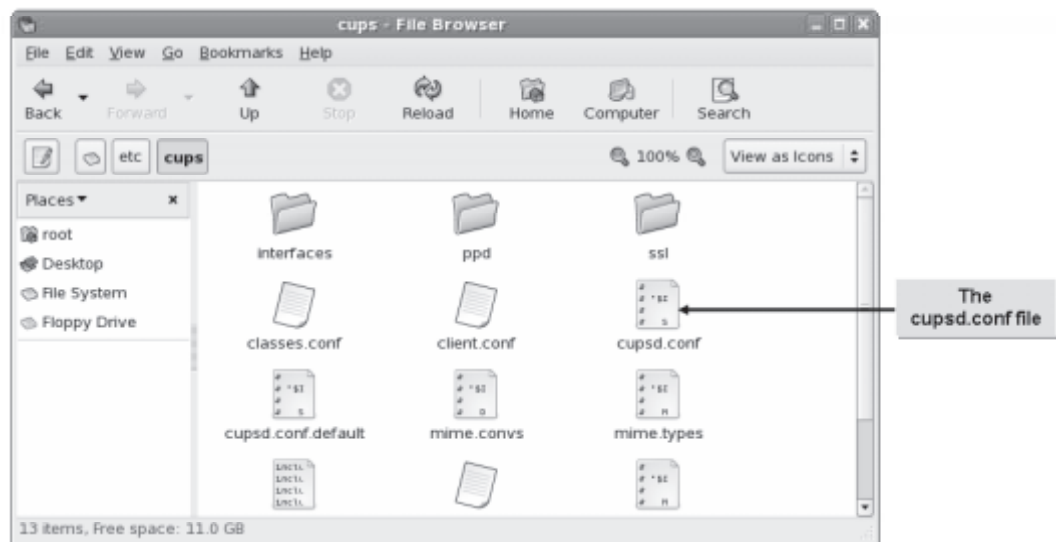


Figure 6-4: Accessing the `cupsd.conf` file located in the `/etc/cups` directory.

The Print Process

The print process enables you to print a document. Various steps are involved in this process. When a user issues a command to print a document in an application, the following steps take place:

1. The application invokes the printing client software.
2. The file passes from the printing client to the printer *spooler*.
3. The file then passes through a number of filters that convert the document from one format to another, before being finally sent to the printer.
4. The printer then prints the file.

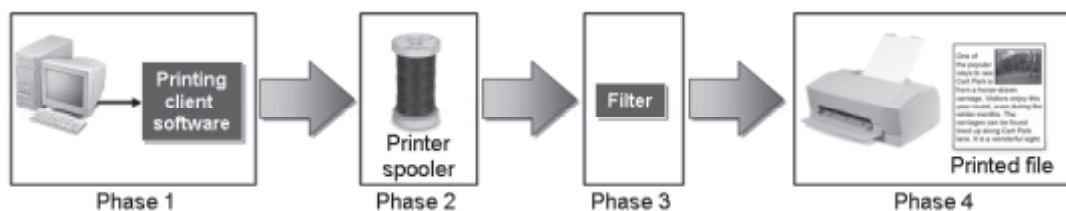


Figure 6-5: Process involved in printing a document.

Spooling

Spooling is the procedure by which print jobs are temporarily stored. If the printer is busy, print jobs are placed in a waiting line or print queue. These jobs are stored in a temporary storage space called a *spool*. Files in the queue are printed when the printer becomes free. This prevents programs from having to wait during a slow printing process.

Print Queues

Definition:

A *print queue* is a temporary storage area that sorts incoming print jobs. Print queues are used by the print daemon so that applications that need to use the printer do not have to wait to issue the command for printing until the current print job is completed. A list of print jobs contains details of the file being printed currently and the files yet to be printed. Print queues allow multiple users to share a printer.

Example:

```

root@localhost:~
File Edit View Terminal Tabs Help
[root@localhost ~]# lpq
printer is ready and printing
Rank  Owner  Job   File(s)                Total Size
----  -
1st   root    12    (stdin)                 1024 bytes
2nd   root    13    (stdin)                 1024 bytes
3rd   root    14    (stdin)                 1024 bytes
4th   root    15    (stdin)                23552 bytes
5th   root    16    (stdin)                 2048 bytes
6th   root    17    (stdin)                 1024 bytes
7th   root    18    (stdin)                 2048 bytes
8th   root    19    (stdin)                 1024 bytes
9th   root    20    (stdin)                23552 bytes
[root@localhost ~]#
  
```

Figure 6-6: Print jobs in a queue.

How to Configure a Local Printer

Procedure Reference: Add a Printer Using the Printer Configuration Dialog Box

To add a printer using the **Printer configuration** dialog box:

1. Connect the printer to the LPT1 port. Switch on the printer and load paper.
2. Log in as root in the GUI.
3. Open the **Printer configuration** dialog box.
 - On the terminal, enter `system-config-printer`.
 - From **Panel**, choose **System→Administration→Printing**.
4. In the Printer configuration - localhost window, on the toolbar, click **New Printer**.
5. In the **New Printer** dialog box, in the **Printer Name** text box, enter the name of the printer.
6. If necessary, in the **Description** text box, enter the description of the printer.
7. If necessary, in the **Location** text box, enter the location details of the printer.
8. To continue with the printer installation, click **Forward**.
9. To install the printer, in the **Select Connection** list box, in the **Devices** list box, select the printer device and click **Forward**.
10. In the **Makes** list box, select the printer make and click **Forward**.
11. In the **Models** list box, select the corresponding model, and in the **Drivers** list box, select the corresponding driver and click **Forward**.
12. To add a new printer, on the confirmation page, click **Apply**.
13. To close the **Printer configuration** dialog box, from the menu, choose **File→Quit**.

Procedure Reference: Add a Printer Using the CUPS Browser Interface

To add a printer using the CUPS browser interface:

1. If necessary, to shift to the GUI, press **Ctrl+Alt+F7**.
2. To launch the web browser, in **GNOME Panel**, click the **Web Browser** icon.
3. In the Address bar, double-click the existing address to select it.
4. To launch the CUPS browser interface, enter `localhost:631`.
5. On the **Home** tab, in the **Welcome** section, click **Add Printer**.
6. On the **Add Printer** web page, in the **Add New Printer** section, in the **Name**, **Location**, and **Description** text boxes, type the name, location, and description of the printer, respectively. Click **Continue**.
7. To configure a local printer, on the **Administration** tab, in the **Device for {printer name}** section, from the **Device** list, select **LPT #1**. Click **Continue**.
8. In the **Make/Manufacturer for {printer name}** section, in the **Make** list box, select the manufacturer of the printer. Click **Continue**.
9. In the **Model/Driver for {printer name}** section, in the **Model** list box, select the model number of your printer and click **Add Printer**.

- 10. In the **Authentication Required** dialog box, enter the root user name and password. Click **OK**.
- 11. If necessary, on the **Set Printer Options** web page, modify the settings as required and close the CUPS web browser interface.

ACTIVITY 6-1

Configuring a Generic Printer

Before You Begin:

- 1. Switch to the GUI.
- 2. The printer is connected to the parallel port (LPT1) of the system and is switched on.
- 3. Paper is loaded in the printer.

Scenario:

You want to print files from your Linux system. However, you have not configured a printer. You have already physically attached a compatible printer, and now you need to configure it.

What You Do	How You Do It
1. Add a printer to the Linux system.	<ul style="list-style-type: none">a. Choose System→Administration→Printing.b. To add a printer, in the Printer configuration - localhost dialog box, click New Printer.c. In the New Printer dialog box, in the Printer Name text box, type <i>printer1</i> and press Tab.d. In the Description text box, type <i>Test</i> and press Tab.e. In the Location text box, type <i>Lab</i> and click Forward.

LESSON 6

2. Select the make and model of the printer to be configured.
 - a. In the **Devices** list box, ensure that **LPT #1** is selected and click **Forward**.
 - b. In the **Makes** list box, ensure that **Generic** is selected and click **Forward**.
 - c. In the **Models** list box, scroll down and select **PostScript Printer**.
 - d. In the **Drivers** list box, select the **foomatic: Generic - PostScript_Printer -Postscript.ppd (recommended)** option and click **Forward**.
 - e. On the confirmation page, observe that the message "Going to create a new printer printer1 at parallel:/dev/lp0." is displayed. Click **Apply** to add the printer.

 3. Check whether **printer1** has been added to the **Local Printers** list and make it the default printer of your system.
 - a. Observe that **printer1** is added to the **Local Printers** list.
 - b. In the **Server Settings** section, click **printer1**.
 - c. To make **printer1** the default printer of your system, on the **Settings** tab, in the **Default Printer** section, click **Make Default Printer**.
 - d. Close the **Printer configuration - localhost** dialog box.
-

ACTIVITY 6-2

Configuring a USB Printer in Linux

Before You Begin:

- 1. You have logged in as root in the GUI.
- 2. The USB printer is connected to the USB port of the system and is switched on.
- 3. Paper is loaded in the printer.

Scenario:

As a system administrator, you are asked to set up a printer in the Linux environment for the HR department. You identified that a USB printer is to be used for this purpose.

What You Do	How You Do It
1. Check the printer configuration.	<ul style="list-style-type: none">a. Choose System→Administration→Printing.b. In the Printer configuration - localhost window, observe that in the Local Printers section, the USB printer is listed as it is automatically added.c. Select <i>{printer name}</i>.d. To make it the default printer, on the Settings tab, in the Default Printer section, click Make Default Printer.e. Observe that the message "This is the default printer" is displayed.

2. Print the test page.
 - a. Click **Print Test Page** to print a test page.
 - b. Observe that a message box is displayed with the text "Test page submitted as job {*job number*}."
 - c. To print the test page, click **OK**.
 - d. Collect the hard copy of the test page and file it.
 - e. To cancel other tests, click **Cancel Tests**.
 - f. Close the Printer configuration - localhost window.

TOPIC B

Print Files

In the last topic, you configured a compatible printer to work with a Linux system. With the printer installed, you are ready to print files. In this topic, you will print files in the Linux system.

Printing a file is a routine task. Learning to print in Linux will save you time when documenting system information and changes. While you can print from the GUI, learning to print from the command line will give you greater freedom when printing from another location.

Printer Commands

Linux comprises various commands that facilitate the printing process. Some of the commands are described in the following table.

Command	Description
lp	Submits files for printing or alters a pending print job. The syntax of this command is <code>lp [options] {file name}</code> .
lpr	Submits files for printing. Files entered on the command line are sent to the specified printer or to the print queue if the printer is busy. If no files are entered on the command line, the <code>lpr</code> command reads the print file from the standard input. The syntax of this command is <code>lpr [options] [file name]</code> .
lpq	Displays the current print queue status. The syntax of this command is <code>lpq [options] {print queue name}</code> .

Command	Description
<code>lprm</code>	Cancels print jobs in the queue. The syntax of this command is <code>lprm {print job id}</code> .
<code>lpc</code>	Allows you to start or stop a printer, enable or disable queues, manage jobs in the queue, and obtain a status report on the printers and queues. The syntax of this command is <code>lpc [parameter]</code> .
<code>lpstat</code>	Displays the CUPS status information. The syntax of this command is <code>lpstat [options]</code> .
<code>cancel</code>	Deletes a print job from the print queue. The syntax of this command is <code>cancel [options]</code> .

The lpr Command

The `lpr` command comprises various options that allow you to specify the nature of the print output.

The `lpr` command options are described in the following table.

Option	Used To
<code>-E</code>	Force encryption when connecting to the server.
<code>-P {destination}</code>	Print files with the destination printer specified.
<code>-# {copies}</code>	Set the number of copies to print from 1 to 100.
<code>-C {name}</code>	Set the job name.
<code>-l</code>	Specify that the print file is already formatted and sent without being filtered to the destination.
<code>-o {option}</code>	Set a job option.
<code>-p</code>	Specify that the print file needs to be formatted with a shaded header that includes the date, time, job name, and page number of the file.
<code>-r</code>	Specify that the print files should be deleted after printing.

The lpc Command

The `lpc` command comprises various options that allow you to manage print jobs.

The pr Command

The `pr` command formats files before they are printed. By default, the `pr` command sends its output to the terminal screen. It is also used in combination with commands that send output to a printer. The `pr` command formats the file's header containing the page number, file name, date, and time.



Figure 6-7: Printing a document using the `pr` command.

Syntax

The syntax of the `pr` command is `pr [options] {file name}`.

pr Command Options

There are many formatting options available for use with the `pr` command.

Option	Description
-{column}	Produces a multi-column output with the data arranged in columns.
-d	Produces a double-spaced output.
-m	Merges files.
-F	Ensures that the pages of the printout are separated by form feeds instead of new lines that include a 3-line page header on pages.
-l [#]	Changes the page length of the output, where # is the number of lines per page.
-h [new header text]	Allows you to change what is included in the header at the top of each page, where [new header text] replaces the file name in the default header contents.

Using pr with Piping

When you format your output with the `pr` command, you can send the formatted output to a file to be printed using the redirection operator (`>`) and pipe. For example, `pr -l45 sales > sales.out` creates the `sales.out` file, which is formatted and ready for printing. In addition, you can send the formatted file directly to the printer using the `lpr` command. For example, the `pr -l45 sales | lpr` command sends the formatted sales file directly to the default printer.

How to Print Files

Procedure Reference: Print a File Without Text Formatting

To print a file without text formatting:

1. Change to the directory that contains the file you want to print.
2. Print the file using the `cat {file name} | lpr` command.

Procedure Reference: Print a File with Text Formatting

To print a file with text formatting:

1. Change to the directory that contains the file you want to print.
2. To view the file with text formatting, enter `pr [options] {file name} | more`.
3. To print the file with text formatting, enter `pr [options] {file name} | lpr`.

ACTIVITY 6-3

Formatting Text for Printing

Before You Begin:

1. You have logged in as root in the GUI.
2. Display the terminal window.

Scenario:

Due to recent changes in the boot process and a hard disk upgrade, you want to print copies of system files for record keeping. Any further change to these files should be documented and a new version should be printed. You decide to use text formatting features to fix any alignment issue before printing the files.

LESSON 6

What You Do	How You Do It
1. Display the contents of the <code>/etc/fstab</code> and <code>/etc/inittab</code> files using the <code>more</code> command.	<ol style="list-style-type: none">To view the contents of the <code>/etc/fstab</code> file, enter <code>more /etc/fstab</code>Observe that the contents of the <code>/etc/fstab</code> file are displayed on the screen.To view the contents of the first page of the <code>/etc/inittab</code> file, enter <code>more /etc/inittab</code>To view the next page of the <code>/etc/inittab</code> file, press the Spacebar.Observe that the contents of the <code>/etc/inittab</code> file are displayed on the screen.To view the remaining part of the file, press the Spacebar.
2. Display the <code>/etc/inittab</code> file using the <code>pr</code> command.	<ol style="list-style-type: none">Enter <code>pr /etc/inittab more</code>Observe that the date, title, and page number are displayed.To view the next page of the <code>/etc/inittab</code> file, press the Spacebar.To view the remaining part of the file, press the Spacebar. Observe the contents of the <code>/etc/inittab</code> file as displayed on the screen.
3. Preview the <code>/etc/fstab</code> file with double line spacing and the heading "The fstab entries."	<ol style="list-style-type: none">To preview the formatting applied to the file, enter <code>pr -d -h "The fstab entries" /etc/fstab more</code>Observe that "The fstab entries" is displayed as the heading and the file has double spacing between the lines.To close the preview and return to the command prompt, press Q.

4. Preview the `/etc/inittab` file contents, 30 lines at a time, using the `pr` command.
 - a. Enter `pr -130 /etc/inittab | more`
 - b. To view the next page of the `/etc/inittab` file, press the **Spacebar**.
 - c. To view the remaining parts of the file, press the **Spacebar**. Observe the contents of the `/etc/inittab` file as displayed on the screen.
 - d. To clear the terminal, enter `clear`
-
5. Print the `/etc/inittab` file with text formatting and the `/etc/fstab` file with and without text formatting.
 - a. To print the `/etc/inittab` file, 30 lines per page, enter `pr -130 /etc/inittab | lpr`
 - b. To print the `/etc/fstab` file with "The fstab entries" as the heading and with double line spacing, enter `pr -d -h "The fstab entries" /etc/fstab | lpr`
 - c. To print the file without formatting, enter `cat /etc/fstab > lpr`
-

TOPIC C

Manage Print Jobs and Queues

Now that you can print files, you need to control the information sent to a printer. In this topic, you will manage print jobs and print queues.

In the earlier versions of Linux operating systems, you were only able to send files directly to a printer. With the advent of updated drivers and printers with more memory, you can now send files directly to a printer and manage the print jobs with the help of a print queue. You can view, edit, and cancel print jobs in the print queue. You can also send high priority jobs for printing ahead of low priority jobs.

The `printtool` and `printconf` Commands

The `printtool` and `printconf` commands provide a graphical interface for setting up a printer queue.

Command	Description
<code>printtool</code>	Used in Red Hat Linux desktop versions, 7.1 and earlier, to set up and configure both local and remote printers. It also allows you to configure Windows SMB printers.
<code>printconf</code>	Used to accomplish the same tasks as <code>printtool</code> in Red Hat Linux desktop versions 7.2 and later.



Red Hat Linux 7.x versions were the predecessors to the Fedora Core series.

How to Manage Print Jobs and Queues

Procedure Reference: Manage Print Jobs in the Print Queue in the CLI

To manage print jobs in the print queue in the CLI:

1. Log in as a user in the CLI.
2. Manage jobs in a queue.
 - To add a job to the print queue, enter `lpr {file name}`.
 - To add a job to a specific print queue, enter `lpr -P {print queue name} {file name}`.
 - To view all the print jobs in the queue, enter `lpq`.
 - To view the print jobs in a specific print queue, enter `lpq -P {print queue name}`.
 - To remove the desired print job, enter `lprm {print job id}`.

ACTIVITY 6-4

Managing Print Jobs and Queues

Data Files:

- Software_List.txt

Before You Begin:

1. You have logged in as root in the GUI. The terminal window is displayed.
2. Enter `cp /085099Data/Printing_Files/* /root`.
3. To clear the terminal window, enter `clear`.
4. To print the list of installed packages, enter `rpm -qai | lp &`.
5. To print the list of available packages, enter `ls -l /rhelsource/Server/* | lp &`.
6. To clear the terminal window, enter `clear`.

Scenario:

You want to print the list of software applications required for your organization. You decide to connect to the local printer and print the file. You also decide to view the print queue to check the status of your file. Because the printout is needed immediately, it has to be printed first.

LESSON 6

What You Do	How You Do It
1. Cancel the jobs in the print queue.	<ol style="list-style-type: none">To view the jobs in the print queue, enter lpqObserve that the files with job ids {job id 1} and {job id 2} are in the print queue.To cancel the job with id {job id 1}, enter lprm {job id 1}To cancel the job with id {job id 2}, enter lprm {job id 2}To view the jobs in the print queue, enter lpqObserve that there are no jobs in the queue. Minimize the root@srvA window.Observe that two message boxes are displayed with the message "Printing of (stdin) on printer {printer name} was cancelled" for each of the canceled jobs. To close both the message boxes, click Close two timesMaximize the root@srvA window.
2. Add a new job to the print queue.	<ol style="list-style-type: none">To add the new job to the print queue, enter lpr Software_List.txtObserve that the first job was only partially printed. The Software_List.txt file is printed.To close the terminal window, enter exit

TOPIC D

Configure Remote Printing

Now that you managed your local printer jobs and queues, you will now be able to apply those print techniques over a network. In this topic, you will connect and use remote printers.

Businesses and home users set up networks to transfer files. With this infrastructure in place, printing across networks is feasible. Being able to print with a remote printer allows you to minimize the number of printers required in your environment. You can have one printer for a larger number of users to share.

Print Servers

Definition:

A *print server* is a computer that enables a network of users to access the central printer. The print server acts as a buffer, storing information to be printed until the printer is free. Print servers can be programmed to print jobs in the order in which they are received or in the order of priority.

Example:

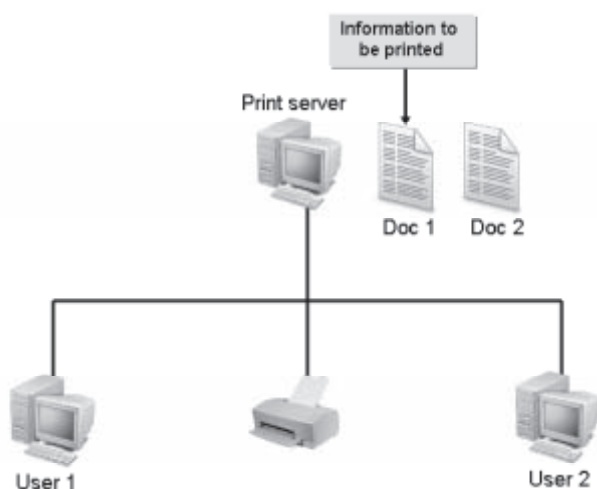


Figure 6-8: A print server manages print jobs over a network.

Remote Printing

In a network environment, users of a Linux system can print files using remote printers through the Linux print system. When you enter the `lpr` command, the file you specify is copied into the remote spool directory where it waits until the remote print server can print it.

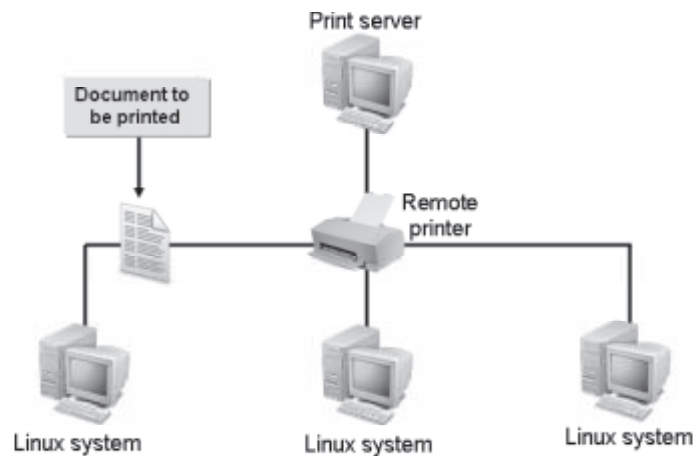


Figure 6-9: *Printing on a network via the Linux print system.*

Syntax

The syntax to print a document remotely is `lpr -P [printer name] [file name]`, where `[printer name]` is the name of the remote printer and `[file name]` is the name of the file you want to print.

Remote Printer Permissions

If you are setting up a remote printer, ensure that your system has the correct permissions to access the remote printer. The permissions are specified in either the `/etc/hosts.lpd` file or the `/etc/hosts.equiv` file, on the system to which the printer is attached. These files list the names of the remote systems that can use the local printer and can be modified to add or remove access to the printer.

Managing Remote Print Jobs

Just as you can manage local print jobs, such as removing jobs from a queue, holding jobs, or reordering jobs, you can also manage remote print jobs. You may not be able to do this as a regular user and may require someone with administrative access to the remote printer to do this for you. However, you should be able to hold or delete your own jobs.

Samba

Samba is a suite of network sharing tools that help in the sharing of files and printers on a heterogeneous network, which consists of computers running on different operating systems. Samba is an open source software application that provides enhanced interoperability with better performance and minimal maintenance. Using the Server Message Block (SMB) protocol, Samba enables Linux systems to communicate with computers running on other operating systems and share network resources such as printers.



Figure 6-10: Samba allows a Linux system to access a printer connected to a Windows operating system.

The Samba Server

Samba allows Linux to emulate some services that a Windows server provides. It allows a user to share resources between Linux and Windows machines. Samba also provides enhanced network security by allowing Active Directory (AD) support. AD helps provide authenticated user access and restricted access permissions. By using shared network resources, you can make printing in AD easy and secure.

The SMB Protocol

SMB is a client-server protocol that is used to share and transfer files on a network. It allows a client on the network to send, print, or scan requests to the server. The server in turn, makes the device available to the client. SMB is mostly used in computers that have Windows operating systems.

Configuring Samba

To configure Samba, you must edit the `/etc/samba/smb.conf` file. The following configuration options must be set in the file:

```
load printers = yes
printing = cups
printcap name = cups
```

In the `[printers]` section, you should have something similar to the following:

```
[printers]
comment = All Printers
path = /var/spool/samba
browseable = no
public = yes
guest ok = yes
writeable = no
printable = yes
printer admin = root, @ntadmins
```

After modifying the file, the Samba service must be restarted for the changes to take effect.

The printers.conf File

The `printers.conf` file, which is stored in the `/etc/cups` directory, defines the set of local printers on a network as shared resources. The list of printers gets generated automatically using the `cupsd` daemon. It can be configured in such a way that it allows only the explicitly publicized printers. The file contains a set of directives that define the features of the printer being shared.

How to Configure Remote Printing

Procedure Reference: Install Samba

To install Samba:

1. Log in as root in the GUI.
2. Mount the Linux installation CD-ROM that contains the latest version of samba packages.
3. Navigate to the /media/[name of the media]/Server folder.
4. Select the samba {package version}.rpm and perl - Convert -ASN1 - {package version}.rpm files.
5. Right-click and choose **Open with Software Installer**.
6. In the Installing packages window, verify that the two packages are listed and click **Apply** to start installing the packages.
7. If necessary, to install the two packages, in the **Unable to verify {package name}** message box, click **Install anyway**.
8. To complete the installation, in the **Software installed successfully** message box, click **OK**.

Procedure Reference: Share a Printer Using Samba

To share a printer using Samba:

1. Open the /etc/samba/smb.conf file.
2. Define a share for a printer.
 - Specify the share name within brackets.
[share name]
 - Define the path to the spool file.
path = {path to the spool file}
 - Specify the printer name.
printer = {printer name}
 - Specify if the guest users are allowed to print. *public = {yes | no}*
 - Specify the printing access for users. *printable = {yes | no}*
 - If necessary, include a comment describing the shared printer. *comment = {Printer Description}*
3. Save and close the file.
4. To verify that the smb.conf file is formed, enter `testparm /etc/samba/smb.conf`.
5. To start the service when the system boots, enter `chkconfig smb on`.
6. To restart the Samba service, enter `service smb restart`.
7. To view the IP address of the system to which the printer is connected, enter `ifconfig`.
8. Verify that the printer share you created is accessible from other Linux systems.

ACTIVITY 6-5

Configuring Remote Printers

Before You Begin:

1. On srvA, you have logged in as root in the GUI.
2. Double-click the **Computer** icon on the desktop.
3. Navigate to the /rhelsource/Server folder.
4. In the Server - File Browser window, navigate and select the perl - Convert - ASN1 - 0.20 - 1.1.noarch.rpm and samba - 3.0.33 - 3.7.el5.i386.rpm files.
5. Right-click and choose **Open with "Software Installer."**
6. In the Installing packages window, verify that the two packages are listed and click **Apply** to start installing the packages.
7. In the **Software installed successfully** message box, click **OK** to complete the installation process.
8. Close the Server - File Browser window.
9. Choose **System**→**Administration**→**Printing** to display the Printer configuration - localhost window.
10. In the left pane, select **Server Settings**.
11. In the right pane, in the **Basic Server Settings** section, check the **Share published printers connected to this system** check box.
12. Click **Apply**.
13. Close the Printer configuration - localhost window.
14. Choose **Applications**→**Accessories**→**Terminal** to launch the terminal window in the GUI.

Scenario:

You configured a local printer on your Linux system. Because you have a number of documents that need to be printed from other Linux systems, you decide to make the printer a shared printer and enable remote access to it with permission granted to the jsmith user account.

LESSON 6

What You Do	How You Do It
1. Modify the smb.conf file to share the printer.	<ol style="list-style-type: none">To open the smb.conf file in the text editor, in the terminal window, enter vi /etc/samba/smb.confNavigate to the Share Definitions section.Navigate to the beginning of the line containing the <i>browseable</i> variable in the printers section.To change to insert mode, press I. To insert a new line before the current line, press Enter and then press Tab.To move to the previous line, press the Up Arrow key and press Tab.Type printer name = printerPress the Down Arrow key and press Backspace two times.To make it browseable, type yes and press the Down Arrow key. Press Backspace two times.To allow the guest account to access the printer share, type yesTo return to command mode, press Esc. Save the file and quit the editor.
2. Add a new smb user and restart the smb service.	<ol style="list-style-type: none">To add jsmith to the list of smb users, enter smbpasswd -a jsmithTo set a blank password, press Enter two times.To view the IP address of the Linux system, enter ifconfigNote down the IP address of the system.To restart the Samba server, enter service smb restart

3. Access the remote printer.
 - a. On srvB, log in as **root** in the GUI.
 - b. Choose **System**→**Administration**→**Printing**.
 - c. To add a printer, in the **Printer configuration - localhost** dialog box, click **New Printer**.
 - d. In the **New Printer** dialog box, in the **Printer Name** text box, type **printer1** and press **Tab**.
 - e. In the **Description** text box, type **Remote Printer** and press **Tab**.
 - f. In the **Location** text box, type **Printer on srvA** and click **Forward**.
 - g. In the **Devices** list box, observe that **LPT #1** is selected.
 - h. Select the **Windows Printer via SAMBA** option.
 - i. In the right pane, observe that the **MYGROUP** share is displayed.
 - j. Double-click the **MYGROUP** share.
 - k. In the right pane, observe that **SRVA** is displayed.
 - l. Double-click the **SRVA** share.
 - m. In the right pane, observe that the printer is displayed.
 - n. Select the printer.
 - o. Observe that in the **smb** section, the printer path is filled in the text box. Click **Forward**.
-

LESSON 6

4. Select the printer driver and set the remote printer as the default printer.
 - a. In the **Makes** list box, ensure that **Generic** is selected and click **Forward**.
 - b. In the **Models** list box, scroll down and select **PostScript Printer**.
 - c. In the **Drivers** list box, select the **foomatic: Generic - PostScript_Printer -Postscript.ppd** option and click **Forward**.
 - d. On the confirmation page, observe that the message "Going to create a new printer printer at smb://MYGROUP/SRVA/printer" is displayed.
 - e. To add the printer, click **Apply**.
 - f. Observe that in the **Remote Printers** section, a new printer, printer@192.168.0.2, is added.
 - g. To set printer1 as the default printer, in the left pane, select **printer1**, and in the right pane, click **Make Default Printer**.
 - h. Observe that printer1 is set as the default printer.
 - i. Close the **Printer configuration - localhost** dialog box.
-

5. Print the `install.log` file on the remote printer.
 - a. On the desktop, double-click the **root's Home** folder.
 - b. In the root window, double-click the **install.log** file.
 - c. To print the file, choose **File→Print**.
 - d. In the **Print** dialog box, observe that the remote printer, `printer@srvA`, is selected and click **Print**.
 - e. Switch to `srvA`.
 - f. To launch the Firefox web browser, on the taskbar, click the **Web Browser** icon.
 - g. To view the jobs in the print queue, in the Address bar, select the existing address and enter `http://localhost:631/jobs`
 - h. Click **Show Active Jobs**.
 - i. Observe that the `install.log` file is displayed in the print queue.
 - j. Close the `Jobs CUPS 1.3.7 - Mozilla Firefox` window.
 - k. Switch to `srvB`.
 - l. Close the `gedit` and `root` windows.
-

Lesson 6 Follow-up

In this lesson, you worked with Linux printing services. You configured both local and remote printers, printed files using various printer commands, and managed print jobs and queues. You will now be able to set up printer connections and print backup records of files.

1. What is the benefit of managing print queues?

LESSON 6

2. What are the differences between a local printer and a network printer?

LESSON 7

Managing Packages

Lesson Time*2 hour(s)*

In this lesson, you will manage packages.

You will:

- Manage packages using the RPM package manager.
- Verify packages.
- Upgrade and refresh packages.
- Configure repositories.
- Manage packages using the YUM package manager.
- Manage packages using the Debian package manager.
- Manage packages using source files.
- Manage shared libraries.

Introduction

You explored the basic Linux environment, worked with files, and printed them. Now, you are ready to install packages to facilitate the distribution and installation of software. In this lesson, you will manage packages.

You will need to install software on your system to perform required tasks effectively. To do this, you need to learn about packages and package managers and how to install them on your system. Unless the packages are fully installed, the desired software will not function.

This lesson covers all or part of the following CompTIA Linux+ Powered by LPI certification objectives:

- Topic A:
 - Objective 102.5
- Topic D:
 - Objective 102.5, Objective 110.3
- Topic E:
 - Objective 102.5
- Topic F:
 - Objective 102.4
- Topic H:
 - Objective 102.3, Objective 105.1

TOPIC A

Manage Packages Using RPM

Installing software on your system will increase the capabilities of your computer and enable you to perform a new set of tasks or perform a common set of tasks much faster. You need to know how to manage packages before you install software. In this topic, you will manage packages using the RPM package manager.

As a Linux professional, you will need to install software on systems. Software is a collection of packages. You can install the software only if you know how to add these packages on your system. Even if one package is not installed correctly, the software will not work. Installation of these packages is facilitated by package managers. Therefore, it is necessary to know about packages and package managers.

Packages

Definition:

A package is a collection of classes, functions, or procedures that can be imported as a unit. Packages include all files required to run an application. Each package is compiled specifically for each Linux distribution and type of system. Packages are of different types, depending on the applications for which they are used.

Example:

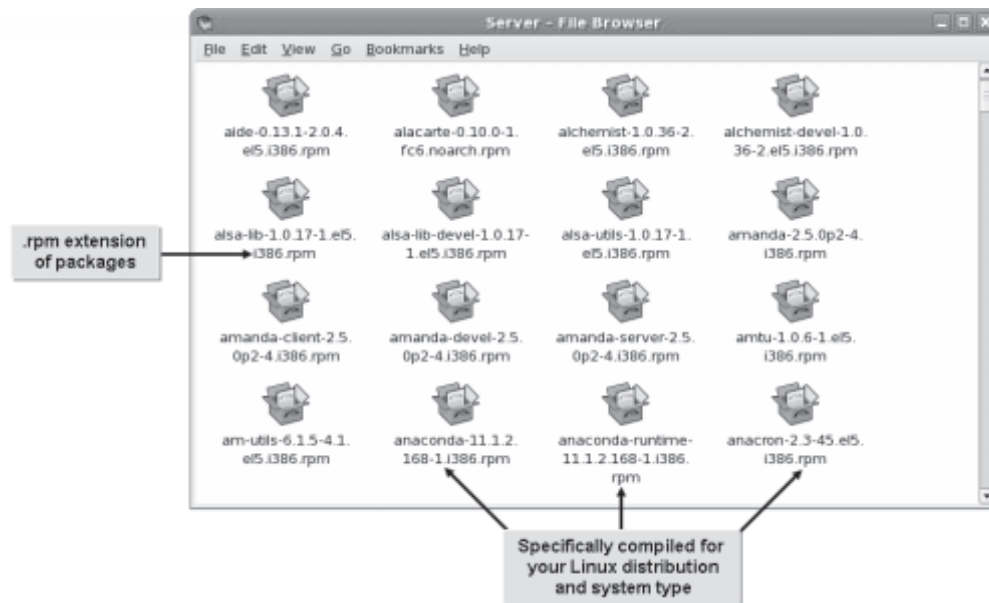


Figure 7-1: Packages on a Linux system.

Package Managers

Definition:

A *package manager* is a tool that enables you to search for packages and upgrade or remove them. It tracks the files that are provided with each package. Querying options are also provided by a package manager to list the installed packages and their characteristics. The naming convention followed by package managers for package files is name-version-release.architecture.rpm. RPM and YUM (Yellow dog Updater, Modified) are examples of package managers.

Example:



Figure 7-2: *Installing a package using the RPM package manager.*

Documenting Changes to Installed Packages

It is recommended that you document any change you make to installed packages. This will help you troubleshoot issues and track the versions that were previously installed.

Dependencies

Dependencies are the packages that a target package depends on for its functionality. Dependency chains can run on for many levels. For example, package A will be installed only after package B is installed. Similarly, package B will be installed only after package C is installed. Package managers can fetch the required packages in an automated manner, saving time and effort. Dependency management is a major function of package managers.


 RPM has several complementary utilities, such as `up2date` and `yum`, to manage dependencies.




Figure 7-3: Package installation fails due to unavailability of dependency packages.

The RPM Package Manager

The *RPM Package Manager (RPM)*, developed by Red Hat, is a tool for maintaining packages. By providing a standard software packaging format, RPM enables easy administration and maintenance of Linux systems and servers. RPM provides a standard installation mechanism, information about installed packages, and a method for uninstalling and upgrading existing packages.



Figure 7-4: Various options of the RPM tool are displayed.

 RPM is distributed under the GNU General Public License (GPL) and can be used with many distributions of Linux and even with other UNIX implementations.

The RPMS Directory

The Red Hat distribution includes the RPMS directory containing packages. You can also find packages on the Internet and FTP sites. One website where you can find packages is <http://rpmfind.net>.

Installing Packages

When you install Linux, you may install all the packages it comes with. However, it is better to install only the packages you need. Later, when you need to install additional packages, you can use your CD or DVD (or whatever source you used) to obtain additional packages. You can check whether the updated versions of the package are released and install a recent version.

The /usr/lib/rpm/* Directory


The /usr/lib/rpm/* directory contains the RPM tools required to manage the RPM packages. The /var/lib/rpm/* directory contains the RPM database of the installed packages. By default, the rpmrc file, which is the global RPM configuration file, is located in the /usr/lib/rpm/* directory. The rpmrc file contains information of the RPM architecture compatibility. If you want the RPM settings to be applicable for a system-wide configuration, place the rpmrc file in the /etc directory. If the rpmrc file is placed as .rpmrc in the home directory of any user, then the RPM settings will be applicable only for that specific user.

RPM Commands

Common RPM package management commands enable you to perform package management tasks.

Frequently used RPM package management commands are given in the following table.

Command	Enables You To
<code>rpm -i {package name}</code>	Install a package.
<code>rpm -F {package name}</code>	Reinstall a package.
<code>rpm -U {package name}</code>	Upgrade a package.
<code>rpm -e {package name}</code>	Remove a package.

 Appending `h` to some of the existing options of the `rpm` command will print 50 hashes as the package archive is unpacked. Appending `v` will give you a verbose status of the package management task that is performed. For example, `rpm -ivh {package name}` will indicate the status of the installation of the RPM package.

RPM Components

The RPM package manager contains a number of components. Using these components, you can maintain a list of packages that are installed on a system.

Component	Description
The RPM local database	Tracks packages that are installed on a system.

Component	Description
The RPM package	Contains many executables and scripts required to install packages.
YUM	Acts as the front-end package installer for RPM.
RPM package files	Contains source code for packages.

RPM Queries

An RPM query is a function that is used to query RPM for information on both installed and uninstalled packages. There are various options, which give distinct outputs, for the `rpm -q` command.



Figure 7-5: Basic details of the samba package obtained using an RPM query.

The options for the RPM query are listed below.

Option	Enables You To
<code>rpm -qa</code>	List all the packages that are installed on your system.
<code>rpm -qc {package name}</code>	List the configuration files of a specified package.
<code>rpm -qi {package name}</code>	Give the basic details of a package such as the installed date, size, signature, and summary.
<code>rpm -ql {package name}</code>	List the files in a package.
<code>rpm -qR {package name}</code>	List the package dependencies.
<code>rpm -qa grep {package name}</code>	Send the results of the rpm query command to the grep command to search the results for a specific package.
<code>rpm -qf {file name}</code>	Find which package provides a specific file.
<code>rpm -qp1 {package name}</code>	List all the files in a package yet to be installed.

Option	Enables You To
<code>rpm -qp {package name}</code>	List the packages that start with a particular alphabet or name. For example, in the syntax, if you substitute <code>{package name}</code> with <code>mysql*</code> , you will get a list of all the packages that start with <code>mysql</code> .

Syntax

The syntax of an RPM query is `rpm -q {what_packages}`
`{what_information}`.

The rpm2cpio Utility

The *rpm2cpio* utility enables you to make a cpio backup of individual files from rpm packages.

How to Manage Packages Using RPM

Procedure Reference: Install Packages

To install packages:

1. Download the rpm file that you want to install.
2. To install the package, use the `rpm -ivh {package name}` command.
3. If necessary, download the dependency packages.

Procedure Reference: Uninstall Packages

To uninstall packages:

1. To search for the rpm package that you want to uninstall, use the `rpm -qi {package name}` command.
2. To uninstall the rpm package, use the `rpm -e {package name}` command.

ACTIVITY 7-1

Managing Packages Using RPM

Data Files:

- AdobeReader_enu-8.1.4-1.i486.rpm

Before You Begin:

1. On srvA, you have logged in as root in the GUI.
2. Display the terminal window.
3. On the terminal, create a directory named rpms in the / directory.
4. Navigate to the /085099Data/Managing_Packages directory. Copy AdobeReader_enu-8.1.4-1.i486.rpm to the /rpms directory.
5. Change to the /rpms directory.
6. To clear the terminal, enter `clear`.

Scenario:

You have a lot of documentation in Linux that is available in the form of ebooks. You need to install the Adobe Reader application to enable users to view the ebooks in Linux.

What You Do	How You Do It
1. Install and check the version of the Adobe Reader package.	<ol style="list-style-type: none"> a. To install the Adobe Reader package, enter <pre>rpm -ivh AdobeReader_enu-8.1.4-1.i486.rpm</pre> b. Observe that the progress bar is at 100% indicating that the package is successfully installed. c. To view the version number of the package, enter rpm -qi AdobeReader_enu d. Observe that the package version is "8.1.4" and the package release is "1."
2. List the files in the Adobe Reader package.	<ol style="list-style-type: none"> a. To view the list of the files in the package, enter rpm -ql AdobeReader_enu b. Observe that the application files are installed in the /opt/Adobe/Reader8/bin directory. c. To clear the terminal window, enter clear

3. Check the status of the files in the Adobe Reader package.
 - a. To view the status of all the files in the package, enter **rpm -qs AdobeReader_enu**
 - b. Observe that the first column displays “normal” as the status for all the files, indicating that the files are correctly installed.
 - c. Minimize the root@srvA: /rpms window.
 - d. On the desktop, double-click the **Adobe Reader 8** icon.
 - e. To accept the terms of the agreement, in the **Adobe Reader - License Agreement** dialog box, click **Accept**.
 - f. Observe that the Adobe Reader window is displayed, indicating that the application is successfully installed.
 - g. Close the Adobe Reader window.
 - h. Restore the root@srvA: /rpms window.
 - i. To clear the screen, in the root@srvA: /rpms window, enter **clear**
-

TOPIC B

Verify Packages

In the last topic, you managed packages using the RPM package manager. As a Linux system administrator, you may have to verify and repair corrupt packages. In this topic, you will verify packages.

As a Linux administrator, you may face situations where due to accidental deletion of important files, the installed packages may stop working. Generally, in such situations, you may need to spend time to identify the missing files and troubleshoot package installations. Because there are a number of packages on the Linux system, it becomes difficult to individually identify the corrupted packages. You can use the rpm package management tools to easily locate such corrupted packages and save time.

RPM Verification

RPM verification compares the existing packages with the RPM package database and returns the missing or corrupt packages. Various options allow you to verify specific information in the package.



Figure 7-6: RPM is used to verify the state of the Samba package.

RPM verification options are listed below.

Option	Enables You To
<code>rpm -Va</code>	Verify all the installed packages.
<code>rpm -V {package name}</code>	Verify a specific package.
<code>rpm -V -f {file name}{package name}</code>	Verify a specific file in the package.

Syntax

The syntax for RPM verification is `rpm -V {package name}`.

Importance of Verifying Packages

The integrity of a package can also be verified via the RPM system. This verification process can be used to ensure that the package files are present in the correct directories without modifications and have the proper permissions. More specifically, RPM checks the size, MD5 checksum, permissions, type, owner, and group of each file in the package.



MD5 checksum is like a file's finger print; it can be used to uniquely identify the file and verify its integrity.

Verification Error Codes

You can check either a specific package or all the packages. If everything is fine with the packages, no messages are displayed and you return to the command prompt. If a problem is detected, an eight-character string is displayed to alert you of the change. Based on this output, you can determine if the package needs to be reinstalled. In the following table, the verification error codes are listed in the same order in which they appear in case there is an error during package verification.

Error Code	Description
S	Change in file size since installation.
M	Different permission or file type mode.
5	MD5 checksum test failed.
D	Device attribute error.
L	Symbolic link errors.
U	Different user setting from the original.
G	Different group setting from the original.
T	Current file modification time does not match the original file modification time.

Any of the eight characters appearing in the output will indicate that the particular test has failed. A period (.) will be displayed if the test is successful. A question mark (?) will be displayed if a test is skipped by the command.

How to Verify Packages

Procedure Reference: Verify Packages

To verify packages:

1. Log in as root.
2. Verify installed packages.
 - To verify all the rpm packages, use the `rpm -Va` command.
 - To verify an individual rpm package, use the `rpm -Vv {package name}` command.
 - To verify a specific file in the package, use the `rpm -V -f {file name} | -p {package name}` command.

ACTIVITY 7-2

Verifying Packages

Before You Begin:

1. You have logged in as root in the GUI.
2. The terminal window is displayed.

Scenario:

Your manager asked you to convert the previously used DOS and Mac files to UNIX format and ensure that the clients are able to access the Samba man pages. After ensuring that the applications are installed, you decide to verify that the packages are ready for use.

What You Do	How You Do It
1. Check whether the dos2unix and samba-client packages are installed.	<ol style="list-style-type: none"> a. To check whether the dos2unix package is installed, on the terminal, enter rpm -q dos2unix b. Observe that the dos2unix - 3.1 - 27.1 package is installed. c. To check whether the samba-client package is installed, enter rpm -q samba-client d. Observe that the samba - client - 3.0.33 - 3.7.el5 package is installed.
2. Verify the dos2unix package.	<ol style="list-style-type: none"> a. To verify the package, enter rpm -Vv dos2unix b. Observe that there are no errors and six lines are displayed.

3. Verify the samba-client package.
- a. To verify the package, enter `rpm -Vv samba-client`

b. Observe that there are no errors and the files are listed followed by the directories.

c. To count the number of files installed with the package, enter `rpm -Vv samba-client | wc -l`

d. Observe that the command displays a total of 26 lines, which indicates that 26 files are part of the samba-client package.

e. To clear the terminal window, enter `clear`
-
-

TOPIC C

Upgrade Packages

Now that you know the methods for verifying packages, you can learn to upgrade packages. In this topic, you will upgrade packages by updating and refreshing installed packages.

One of the aspects of system administration is keeping the system’s software up-to-date. Many applications are in active development and new releases are made available on a regular basis. These new releases may add functionality, fix bugs in older versions, or provide important security updates. RPM has the ability to quickly and easily upgrade software packages. This will save you from having to uninstall and reinstall a package, to have the newest version. Upgrading packages allows you to have the newest features of an application in the shortest amount of time.

Upgrade/Freshen Packages

Packages can be easily upgraded by using the upgrade or freshen option.

Option	Description
Upgrade	Checks package versions against the package versions installed already. If the package is found, the package will be upgraded. If the package is not found, the package will be installed. The syntax that is used to update packages is <code>rpm -U {package name}</code> .

Option	Description
Freshen	Checks package versions against the package versions installed already. If the package is found, the package will be updated. If the package is not found, the package will not be installed. The syntax that is used to freshen packages is <code>rpm -F {package name}</code> .

Freshen Packages

Entering `rpm -Fvh *.rpm` automatically upgrades only those packages that are already installed.

How to Upgrade and Refresh Packages

Procedure Reference: Upgrade Packages

To upgrade packages:

1. Download the updated package.
2. Update the existing package using the `rpm -Uvh {package name}` command.
3. To verify that the package is updated, use the `rpm -qi {package name}` command.

Procedure Reference: Freshen Packages

To freshen packages:

1. Download the updated package.
2. To freshen the existing package, use the `rpm -Fvh {package name}` command.
3. To verify that the package is updated, use the `rpm -qi {package name}` command.

ACTIVITY 7-3

Upgrading Packages

Data Files:

- AdbeRdr9.1.0 - 1_i486linux_enu.rpm

Before You Begin:

1. You have logged in as root in the GUI.
2. Navigate to the /085099Data/Managing_Packages directory. Copy AdbeRdr9.1.0-1_i486linux_enu.rpm to the /rpms directory.
3. To clear the terminal window, enter `clear`.

Scenario:

You installed PDF software on a Linux system to enable users to view ebooks. Some users encounter errors when they try to open the most recent ebooks. After checking the errors, you decide to upgrade the PDF software to the latest version.

What You Do	How You Do It
1. Install the newer version of the Adobe Reader package.	<div>a. To upgrade the Acrobat Reader package, in the terminal window, enter rpm -Uvh AdbeRdr9.1.0-1_i486linux_enu.rpm</div> <div>b. Observe that the progress bar is at 100% for AbodeReader_enu, indicating that the package is successfully installed.</div>

2. Verify that the Adobe Reader package is upgraded.
 - a. To view information about the package, enter **rpm -qi AdobeReader_enu**
 - b. Observe that the package version is "9.1.0" and the package release is "1."
 - c. To change to the bin directory, enter **cd /opt/Adobe/Reader9/bin**
 - d. To launch the application, enter **./acroread**
 - e. To accept the terms of the agreement, in the **Adobe Reader - License Agreement** dialog box, click **Accept**.
 - f. Observe that the Acrobat Reader window is displayed.
 - g. Close the Acrobat Reader window.
 - h. To clear the terminal window, enter **clear**
-

TOPIC D

Configure Repositories

In the last topic, you upgraded and refreshed the installed packages. When managing a network, you may have to update systems with the latest packages. Ultimately, you need to know where to obtain these packages. In this topic, you will examine repositories and how to use them to update systems.

In Linux, there are a number of packages that keep evolving with new versions of the same package being available. As a Linux administrator, you need to ensure that the latest packages are installed on a system by updating only the specific packages instead of reinstalling the entire Linux OS every time. To ensure this, you must know where the packages are available and how they can be downloaded. Updating systems with the latest packages will help users to make use of the newer features of the packages and be able to perform their tasks efficiently.

Repositories

Definition:
A *repository* is a database that holds source code and compilations of Linux software and applications. There are two types of repositories; local and online. Software can be installed on a system only when repositories for the software are present on the system. The packages for the software are found in their respective repositories and are directly installed from them.

Example:

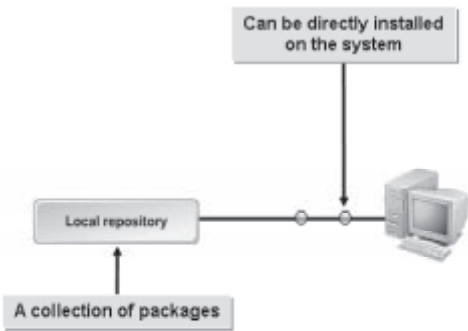


Figure 7-7: A local repository.

Types of Repositories

There are two types of repositories, *online repositories* and *local or private repositories*. Online repositories are found on the Internet. Packages can be directly downloaded from the Internet and installed on a system. Local or private repositories are stored on a system. The process of updating systems is greatly facilitated by repositories because the source files are readily available. Repositories make it easy for system administrators to update multiple systems simultaneously.

The createrepo Command

The *createrepo* command is used to create yum repositories. It generates XML metadata called *repomd* and creates a repository from existing rpm packages.

Various options for the *createrepo* command are listed below.

Option	Enables You To
-p	Generate the output in an XML format.
-s	Select the format of the checksum (such as SHA or MD5) to be used to create a repository.
-c {directory name}	Compare a repository with the checksum and check package integrity. Creates a cache directory for the package checksum.
-x {file name(s)}	Exclude the specified files from a repository.
-h	Show the help menu.
-v	Run the command verbosely.

Syntax

The syntax of the `createrepo` command is `createrepo [options] {directory}`.

How to Configure Repositories

Procedure Reference: Create a Private Repository

To create a private repository:

1. Log in as root.
2. To create a directory, on the terminal, enter `mkdir /{directory name}`.
3. Populate the directory with packages.
4. To create a private repository, enter `createrepo -v /{directory name}`.
5. If you add or remove any package from the directory, run the `createrepo` command again.

Procedure Reference: Configure Additional Repositories

To configure additional repositories:

1. Log in as root.
2. To navigate to the `/etc/yum.repos.d` directory, enter `cd /etc/yum.repos.d`.
3. To create a file, enter `vi {file name}`.
4. Switch to insert mode.
5. Type the required information.
 - To set the repository name, enter `name = repository name`.
 - To give a description of the repository, enter `description of the repository`.
 - To set the repository's base URL, enter `baseurl = {URL of the repository}`.
 - To control the status of the repository, enter `enabled = { 0 | 1 }`.
 - To control the GPG signature verification, enter `gpgcheck = { 0 | 1 }`.
6. Save and close the file.

GPG

GnuPG (GPG) is free software used for encrypting and signing packages or files. The encryption or signature is used to verify the authenticity of any file shared on the network.

ACTIVITY 7-4

Configuring Repositories


Before You Begin:

- 1. You have logged in as root in the GUI.
- 2. The terminal window is displayed.
- 3. To change to the Server directory, enter `cd /rhelsource/Server`.
- 4. To enable gpgcheck in the yum configuration file, change the line `gpgcheck=0` to `gpgcheck=1`. Save the file and exit the editor.
- 5. To clear the terminal window, enter `clear`.

Scenario:

You are assigned the task of updating a few systems on the network with the kickstart application. During installation, you find that there are hundreds of packages in the installation folder, and you have to search for the kickstart packages every time. Therefore, you decide to make your job easier by creating a kickstart repository with specific packages, so that you can call the repository instead of searching for the packages.

What You Do	How You Do It
1. Install the createrepo package.	<ul style="list-style-type: none">a. To install the createrepo package, enter <code>rpm -ivh createrepo-0.4.11-3.el5.noarch.rpm</code>b. Observe that the progress bar is at 100% indicating that the package is successfully installed.c. To verify that the package is installed, enter <code>rpm -q createrepo</code>d. Observe that the "createrepo-0.4.11-3.el5" package is displayed.e. To view information about the package, enter <code>rpm -qi createrepo</code>f. Observe that the package version is "0.4.11" and the package release is "3.el5."

-
2. Create a private repository.
- a. To navigate to the `/` directory, enter **`cd /`**
 - b. To create a private repository, enter **`createrepo -v /rhelsource`**
 - c. Observe that the 2255 packages from the `/rhelsource/Server` directory are entered into the repository.
-  It will take some time to process all the packages.
-
3. Configure the new repository.
- a. To navigate to the `/etc/yum.repos.d` directory, enter **`cd /etc/yum.repos.d`**
 - b. To create the `rhelsource` file, enter **`vi rhelsource`**
 - c. Switch to insert mode.
 - d. To specify the repository name, enter **`name = rhelsource`**
 - e. To specify the repository description, enter **`My Local Repository`**
 - f. To specify the base URL, enter **`baseurl = file:///rhelsource/Server/`**
 - g. To enable the repository, enter **`enabled = 1`**
 - h. To disable `gpgcheck`, type **`gpgcheck = 0`**
 - i. To exit command mode, press **`Esc`**.
 - j. Save and close the file.
-

4. Disable gpgcheck in the yum configuration file.
 - a. To navigate to the yum.conf file, enter **vi /etc/yum.conf**
 - b. To move the cursor to the end of the gpgcheck=1 line, enter **/gpg** and press **End**.
 - c. Switch to insert mode.
 - d. To disable gpgcheck, change **gpgcheck=1** to **gpgcheck=0**
 - e. To exit command mode, press **Esc**.
 - f. Save and close the file.
 - g. To clear the terminal window, enter **clear**
-

TOPIC E

Manage Packages Using YUM

In the last topic, you managed package installation on a single computer using RPM. As a system administrator, your task involves installing software on multiple systems simultaneously within a short period of time. In this topic, you will manage package installation using YUM.

As a system administrator, you will be dealing with multiple systems at the same time. It is necessary that you install packages on all systems simultaneously and in the shortest possible time. Knowledge about the YUM package manager will help you install and manage packages on multiple systems simultaneously.

The YUM Package Manager

Yellow dog Updater, Modified (YUM) is a package manager that is used to update, install, and manage packages. YUM automatically detects and configures the dependencies for software packages and maintains a database of the installed software. YUM is widely used by system administrators because it is easy to work with. It supports both local and online repositories.

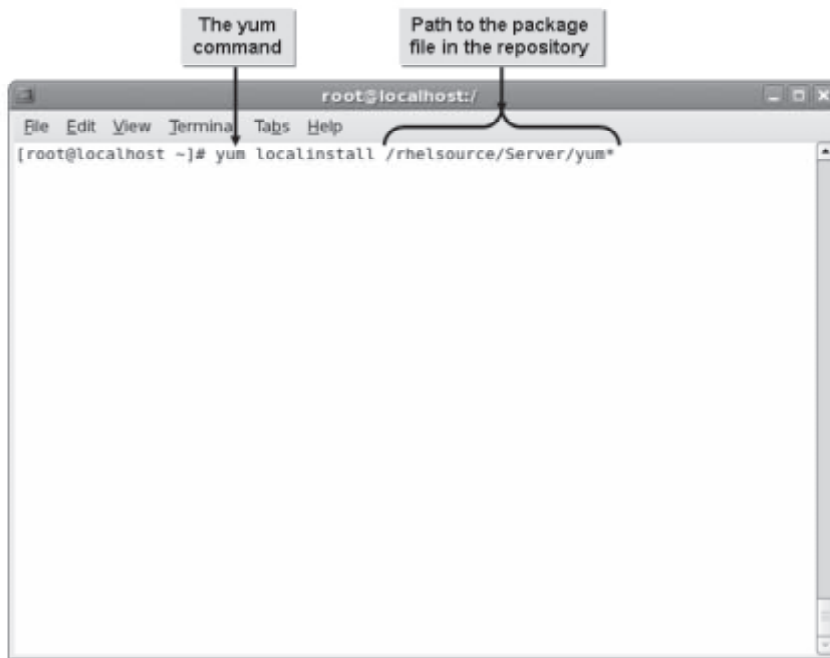


Figure 7-8: Installing a package from a local repository using the YUM package manager.

YUM Commands

YUM has various commands that can be used to maintain packages.

Command	Enables You To
<code>install</code>	Install a package.
<code>update</code>	Update packages. The command will update all packages when a package is not specified.
<code>check-update</code>	Check for available updates.
<code>remove</code>	Remove the specified packages.
<code>list</code>	Display the details of the specified package. When a package is not specified, it lists the status of all the packages on the system.
<code>info</code>	Display a brief description of the specified package.
<code>localinstall</code>	Install packages from a local repository.

Syntax

The syntax of the YUM command is `yum [options] {command} {package name}`.

The yumdownloader Utility

The `yumdownloader` utility allows you to download rpm packages from yum repositories. This utility is part of the `yum-utils` package.

The syntax of the yumdownloader utility is `yumdownloader [options] {package name}`.

How to Manage Packages Using YUM

Procedure Reference: Manage Packages Using YUM

To manage packages using YUM:

1. Log in as root.
2. Manage packages using YUM.
 - To install packages using YUM, enter `yum install {package name}`.
 - To remove packages using YUM, enter `yum remove {package name}`.
 - To display package description, enter `yum info {package name}`.
 - To update the system with the specified package, enter `yum update {package name}`.

ACTIVITY 7-5

Managing Packages Using YUM

Before You Begin:

1. You have logged in as root in the GUI.
2. The terminal window is displayed.
3. To change to the root directory, enter `cd /root`.
4. To clear the terminal window, enter `clear`.

Scenario:

A meeting is scheduled at your company. You are required to install the ypbind service on the systems in the conference room to enable network communication. You are also asked to brief users on the installed ypbind packages. You decide to install the packages and generate a description using the details displayed in the YUM output.

What You Do	How You Do It
1. Install the ypbind package using YUM.	<ol style="list-style-type: none">To install the package, enter <pre>yum localinstall /rhelsource/Server/yp*</pre>To confirm download, at the Is this ok [y/N] prompt, enter yObserve that the dependencies are updated and the "Complete!" message is displayed.To clear the terminal window, enter clear
2. Check the status of the package.	<ol style="list-style-type: none">To view the status of the ypbind package, enter yum list ypbindObserve that "ypbind.i386" is listed under "Installed Packages."To view the description of the ypbind package, enter yum info ypbindObserve that the package version is "1.19" and the package release is "11.el5."To clear the terminal window, enter clear

TOPIC F

Manage Packages Using the Debian Package Manager

In the previous topic, you managed packages using the YUM package manager. You may also need to manage packages in other distributions of Linux, which have their own package managers. In this topic, you will manage packages using the Debian package manager.

As a Linux administrator, you may need to remove obsolete packages to free hard disk space. It will be easier to delete unwanted packages if you know where they are installed. You will need to track all the files that were added during the installation of the packages. This can be done by using the Debian package manager.

The Debian Archive Package Installation Process

The Debian Archive Package Installation process consists of three stages: check for dependency, unpack, and configure.


1. In the *check for dependency* stage, the package manager checks the specified Debian archive package for the numerous dependencies required.
2. In the *unpack* stage, the Debian archive package and its dependent packages are unpacked into the filesystem of the hard disk.
3. In the final *configure* stage, the unpacked files can be configured with the default or customized values to suit your requirements. In addition to this, you can choose to reconfigure the package and its dependencies later.



Figure 7-9: Stages in the Debian Archive Package Installation process.

DEB Tools

DEB tools are a set of tools for package management of Debian-based Linux distributions. DEB tools are used to install, list, and remove packages conforming to the DEB packaging standard.

 The Advanced Package Tool (APT) is a front end for the DEB suite of tools, designed to make it more user friendly.

The tools included in the DEB suite are listed in the following table.

Tool	Description
<code>dpkg</code>	It is the main package management program. Its main purpose is to install and remove DEB packages.
<code>dpkg-deb</code>	It is the archive manipulation tool of the Debian binary package. It is used to extract the DEB package contents from a directory and display package information. It is also used to collect and remove information about Debian archives.
<code>dpkg-reconfigure</code>	It is a tool that allows you to upgrade the installed packages. It enables you to specify options similar to the original installation of the package. Additionally, you can select the front-end interface application for this tool.
<code>dpkg-split</code>	It splits packages into smaller parts. It is useful for splitting packages into sizes of 1.44 MB, so that they can fit into a series of floppy disks.
<code>dselect</code>	It is a menu-driven, front-end interface of the <code>dpkg</code> package. Through this utility, you can install and remove packages.

Debian Archive Package Management Commands

Debian package management commands can be used to get information about Debian archive packages.

These commands have various options.

Option	Used To
<code>dpkg -p [Debian package name]</code>	View the version, dependencies, and integrity of the package.
<code>dpkg -L [Debian package name]</code>	List the contents of the package.
<code>dpkg -l [Debian package name]</code>	View the installation status.
<code>dpkg --yet-to-unpack</code>	Find the packages that are yet to be installed.
<code>dpkg -S [file or package name]</code>	Find packages containing specific files or software.

The apt-get Command

The `apt-get` command is used to install or upgrade packages through the Internet or from the distribution CD. While installing or upgrading packages, the `apt-get` command accesses the website or the CD-ROM listed in the `/etc/apt/sources.list` file.

The `apt-get` command has various options.

Option	Used To
<code>apt-get install {Debian package name}</code>	Install packages.
<code>apt-get remove {Debian package name}</code>	Uninstall packages.
<code>apt-get update</code>	Update the list of new packages available.
<code>apt-get upgrade [Debian package name]</code>	Upgrade packages.

Syntax

The syntax of the `apt-get` command is `apt-get [options] {command}`.

The apt.conf File

The `apt.conf` file is the configuration file for the `apt-get` command. This file stores additional information such as the number of attempts to be made while downloading packages and the available cache memory.

The /var/lib/dpkg/* Directory

The `/var/lib/dpkg/*` directory contains the Debian database of the installed packages. By default, the `dpkg.cfg` file, which is the `dpkg` configuration file, is located in the `/etc/dpkg` directory. The `dpkg` configuration file may contain all the `dpkg` command line options.

aptitude

`aptitude` is a text based front-end tool for the APT package manager. It is used in the same manner as the `apt-get` command.

Alien

Alien is a program in Debian that converts packages in other Linux distribution file formats to Debian. It supports conversion among packages such as Linux Standard Base, RPM, deb, Stampede, and Slackware.

Example of Conversion

The `alien --to-deb {file name}` command will convert an `.rpm` package into a `.deb` package.

How to Manage Packages Using the Debian Package Manager

Procedure Reference: Install Packages Using the Debian Package Manager

To install packages using the Debian package manager:

1. Ensure that Debian Linux is installed on the system.
2. Log in as root in the CLI, or in the GUI display the terminal window.

3. To install the Debian package, on the terminal, enter `dpkg -i {Debian package file}`.

Procedure Reference: Upgrade Packages Using the Debian Package Manager

To upgrade packages using the Debian package manager:

1. Log in as root in the CLI, or in the GUI display the terminal window.
2. Upgrade a Debian package.
 - Enter `dpkg --update-avail {Debian package file}` or;
 - Enter `dpkg-reconfigure {Debian package name}`.

Procedure Reference: Uninstall Packages Using the Debian Package Manager

To uninstall packages using the Debian package manager:

1. Log in as root in the CLI, or in the GUI display the terminal window.
2. To uninstall packages, enter `dpkg -r {Debian package name}`.

Procedure Reference: Manage Packages Using the apt-get Command

To manage packages using the apt-get command:

1. Log in as root.
2. To search for files that match a specific pattern or a specific package, enter `apt-cache search {regular expression}/{package name}`.
3. Manage packages using suitable commands.
 - To install a Debian package, enter `apt-get install {Debian package name}`.
 - If necessary, to update the list of new packages available, enter `apt-get update`.
 - To upgrade a Debian package, enter `apt-get upgrade [Debian package name]`.
 - To uninstall a Debian package, enter `apt-get remove {Debian package name}`.

Procedure Reference: Install Alien Packages Using the alien Command

To install Alien packages using the alien command:

1. Log in as root in the CLI.
2. To install packages belonging to other distributions, type `alien -i {package file name}`.

ACTIVITY 7-6

Managing Packages Using the Debian Package Manager

Data Files:

- Training_Policy.txt

Before You Begin:

1. Reboot srvA and start Debian Linux on the system.
2. Log in as root in the GUI.
3. In the **This session is running as a privileged user** dialog box, click **Continue**.
4. Copy the Training_Policy.txt file.
 - a. On the desktop, double-click the / object.
 - b. In the window, double-click **root**.
 - c. In the root window, double-click the **085099Data** folder.
 - d. In the 085099Data window, double-click the **Managing Packages** folder.
 - e. Copy **Training_Policy.txt** and paste it in the **root's Home** folder on the desktop.
5. Close all open windows.
6. Insert the Debian 5.0.0 i386 Bin-1 disc in the CD drive.
7. Launch the terminal window.
8. To navigate to the less directory, in the terminal window, enter
`cd /media/cdrom/debian/pool/main/l/less.`
9. To copy the less package to the /root directory, enter `cp less_418-1_i386.deb /root.`
10. To clear the terminal window, enter `clear`.

Scenario:

A user, Mike, is trying to view the Training_Policy.txt file on the Debian Linux system. Because the text in the file is several pages long and the content scrolls on the screen, he is having trouble viewing the content of the file. You decide to install the less_418-1_i386.deb package on his system. After installation, you decide to make a note of the version number of the program for documentation purposes.

What You Do	How You Do It
1. Install the less package and view the package version number.	<ol style="list-style-type: none">To change to the root directory, enter cd /rootTo install the less package, enter dpkg -i less_418-1_i386.debObserve that the package is selected, unpacked, and set up, and the man-db is processed.
2. View the Training_Policy.txt file using the less command.	<ol style="list-style-type: none">To view the version number of the less package, enter dpkg -l lessObserve that the version of the less package installed is "418 - 1."To view the first page of the Training_Policy.txt file, enter less Training_Policy.txtTo view the next page of the file, press the Spacebar.Observe that the next page is displayed. To close the file, press Q.To clear the terminal window, enter clear

TOPIC G

Manage Packages Using Source Files

In the previous topic, you managed packages using package managers that are specific to a Linux distribution. You may come across situations where you need to build packages from their source code. In this topic, you will manage packages using source files.

Linux supports different kinds of packages. As a Linux administrator, you need to be aware of the package managers that allow you to handle specific packages. The standard package managers have restrictions in the number of file types they can recognize and, they might also be available only in certain Linux distributions. While it may be possible that you can install the relevant package managers to handle the required file types, the number of file types make it practically impossible. To overcome this, you need to be able to handle generic files, without relying on package managers. As a Linux administrator, your ability to work with source files will give you the skill and flexibility to troubleshoot and manage packages in any Linux distribution. You will be in a position to install applications, regardless of the availability of specific package managers.

makefile

makefile is a description file that contains the details of files, dependencies, and rules with which an executable application is built. It is used to configure, compile, and install the application or driver. System built-in rules for maintaining, updating, and regenerating groups of programs are overridden by the contents of makefile.

Details with which an executable application is built



```

root@localhost:/
File Edit View Terminal Tabs Help
NAME=redhat-rpm-config
VERSION=$(shell awk '/Version:/ { print $2 }' $(NAME).spec)

CVSROOT = $(shell cat CVS/Root 2>/dev/null || :)

CVSTAG = REDHAT_RPM_CONFIG_$(subst .,_,$(VERSION))

all:

tag-archive:
    cvs -Q tag -F $(CVSTAG)

create-archive:
    @rm -rf /tmp/$(NAME)
    @cd /tmp ; cvs -Q -d $(CVSROOT) export -r$(CVSTAG) $(NAME) || echo "Um..
    . export aborted."
    @mv /tmp/$(NAME) /tmp/$(NAME)-$(VERSION)
    @cd /tmp ; tar -czSpf $(NAME)-$(VERSION).tar.gz $(NAME)-$(VERSION)
    @rm -rf /tmp/$(NAME)-$(VERSION)
    @cp /tmp/$(NAME)-$(VERSION).tar.gz .
    @rm -f /tmp/$(NAME)-$(VERSION).tar.gz
    @echo ""
    @echo "The final archive is in $(NAME)-$(VERSION).tar.gz"
  
```

Figure 7-10: *makefile* is used to configure, compile, and install the application or driver.

makefile Commands

makefile allows you to build an application or a driver from its source. You need to issue certain commands in a sequence.

Command	Used To
<code>./configure</code>	Gather system information to compile an application.
<code>make</code>	Compile an application.
<code>make install</code>	Install the newly compiled program.
<code>make uninstall</code>	Uninstall a program.
<code>make clean</code>	Clean up after successfully compiling an application.
<code>make test</code>	Install a perl module. It is an optional command in the package management function.



In the above commands, `make clean` and `make test` are optional, while the first four commands are necessary in any makefile operation.

Autoconf

You can use autoconf to create shell scripts that automatically configure packages. The shell scripts created by autoconf can run independently.

Tarballs

Some applications, even though they are really just standard tar files, are referred to as tarballs. Tarballs come in several different formats, as described in the following table.

Format	Description
<code>.tar</code>	The standard tar file without extra compression.
<code>.tar.gz</code> or <code>.tgz</code>	The standard gzip-compressed tar file.
<code>.tar.bz2</code>	A tar file that is further compressed using the bzip2 utility.
<code>bin.tar</code> , <code>.bin.tar.gz</code> , or <code>.bin.tgz</code>	A tar file containing binary files rather than source files.

Compiling from makefile

Most source files are available in the tarball format. To compile an application, you need to be at the command line or work through a GUI. First, change to the directory that is made by the package. Here, you should find an `INSTALL` file. Read the contents of the `INSTALL` file. Most tarballs include one or more of the following files: `INSTALL`, `COPYING`, `README`, or `CHANGES`. The `INSTALL` file usually includes a generic process for installing tarballs. If a program needs to be compiled in a certain way, you can find the necessary information in either the `INSTALL` or `README` file. This is how it works in theory, but it does not always work, usually due to dependencies on other programs.

makefile and configure Script

Generally, application vendors provide either a makefile or a configure script to build an executable program. Both files come with default settings, and you can customize these files to suit your individual preferences. For example, you can specify the location where you need the files to be installed.

When you build a program using a makefile, you need to make the necessary changes to the file, and you also need to update the necessary header files; otherwise, the installation will be incomplete. When a vendor provides you with a configure script, you can make the desired changes to the script and then run the script. This will generate the necessary files along with the makefile. Because it is not necessary to make any change to the makefile, you can proceed with the installation.

Drivers

A *driver* is a program that controls a device attached to a computer. Linux has a modular kernel, which allows hardware devices to be added to a system without recompiling the kernel as long as the modules for the devices are already compiled. Each driver will have specific instructions on how to create the module and install it. These driver instruction files will also list any dependencies that need to be installed.

How to Manage Packages Using Source Files

Procedure Reference: Compile Applications or Drivers

To compile an application or driver:

1. Download the source code from the vendor.
2. Untar and unzip the files into a directory.
3. In the directory containing the files, issue the `./configure` command.
4. Next, issue the `make` command to compile the application.
5. To install the application, use the `make install` command.
6. To clean up the temporary files used during the compile process, use the `make clean` command.

ACTIVITY 7-7

Managing Packages Using Source Files

Data Files:

- httpd-2.2.11.tar.gz

Before You Begin:

1. Reboot srvA and start Red Hat Linux on the system.
2. Log in as root in the GUI.
3. Display the terminal window.
4. To change to the Managing_Packages directory, enter `cd /085099Data/Managing_Packages`.
5. Copy the httpd-2.2.11.tar.gz file to the /usr directory.
6. To make /usr the current directory, enter `cd /usr`.
7. To clear the terminal window, enter `clear`.

Scenario:

A colleague wants to install the latest version of a web server on a system running Linux. The necessary files have been downloaded, but your colleague needs help in installing the web server from the downloaded source files.

What You Do	How You Do It
1. Extract the source files of the web server.	<div>a. To unzip and extract the file, enter <code>gunzip httpd-2.2.11.tar.gz</code></div> <div>b. To extract the archived files, enter <code>tar xvf httpd-2.2.11.tar</code></div> <div>c. To clear the terminal window, enter <code>clear</code></div>

LESSON 7

2. Configure the web source using the source code.
 - a. To change the directory, enter **cd httpd-2.2.11**
 - b. To configure the httpd source file, enter **./configure --prefix=/etc/apache**
 - c. To clear the terminal window, enter **clear**
 - d. To build the executable program, enter **make**
 - e. To clear the terminal window, enter **clear**
 - f. To install the packages, enter **make install**
 - g. To clear the terminal window, enter **clear**

 3. Start the web server service and verify that the home page is displayed.
 - a. To start the httpd service, enter **./httpd -d /etc/apache/ -k start**
 - b. To launch the web browser from the terminal, enter **firefox http://localhost**
 - c. In the Mozilla Firefox window, observe that the message "It works!" is displayed.
 - d. Close the Mozilla Firefox window.
 - e. To clear the screen, in the terminal window, enter **clear**
-
-

TOPIC H

Manage Shared Libraries

In the last topic, you installed programs from their source. These and all other applications require files and services to function. In this topic, you will manage shared libraries to ensure the proper working of dependent applications.

As a system administrator, you will need to handle system software and also other applications that you install. A number of these applications may require similar services to ensure their proper working. It will be helpful to have these services easily accessible to applications with similar needs. Managing shared libraries can help accomplish this with ease.

Shared Libraries

Definition:

A *shared library* is a file that contains routines, which are used by various applications. Shared libraries are loaded into the memory by the operating system when required. They are then shared with other applications. Shared libraries are loaded when an executable file that links to them is loaded.

Example:

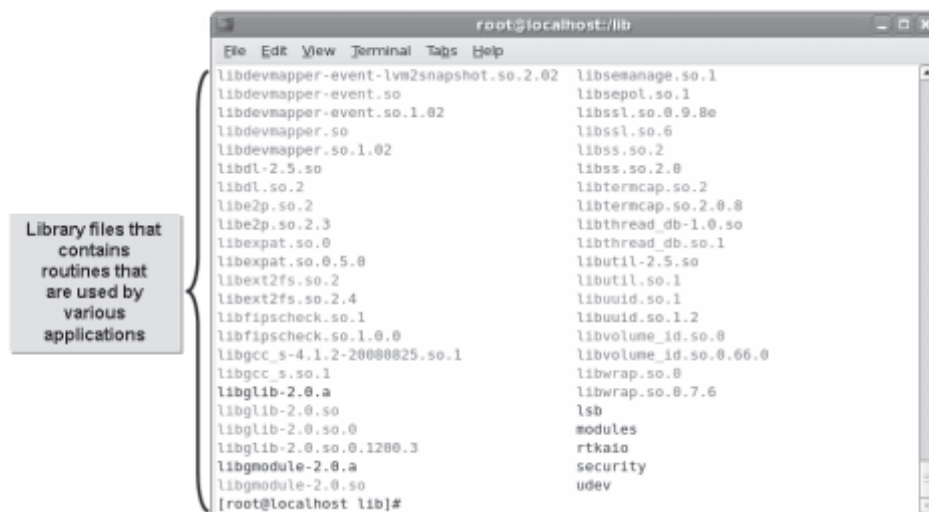


Figure 7-11: List of shared libraries.

Executable Programs

An executable program is a file in a format that a computer can directly execute. Executable files cannot be read by human beings because they are not plain text files and are compiled. An executable file is used to perform various functions or operations on a computer. Binary machine instructions that the computer knows how to execute, can be included in an executable file. It can also contain a shell script. Executable files in Linux can have any name.

How to Manage Shared Libraries

Procedure Reference: Install Library Files

- To install library files:
1. Log in as root.
 2. To identify the library files required for a package to be installed, enter `rpm -qpR {package file name}`.
 3. If necessary, to update the `locate` command database, enter `updatedb`.
 4. To verify that the library files are present on the system, enter `locate {library file name}`.
 5. If the library files are not present, install the necessary packages by entering `rpm -ivh {package file name}`.

Procedure Reference: Determine the Location of Shared Libraries

- To determine the location of shared libraries:
1. Log in as root.
 2. To display the list of shared library required for an application, enter `ldd /{location of the executable file}`.

The ldconfig Command

When you add a new library file, the file details are passed on to the `/etc/ld.so.conf` file, which contains the details of the default system libraries. You need to run the `ldconfig` command to update these changes from the `/etc/ld.so.conf` file and load the shared libraries from the locations specified to the `/etc/ld.so.cache` file. The `/usr/lib` and `/lib` directories are the default system library file locations where the system libraries are kept. Some of the common `ldconfig` command options are given in the following table.

If You Need To	Use This ldconfig Command Option
Specify the configuration file where the library paths are stored.	<code>-f {configuration file name}</code>
Specify the cache file where the library file updates will be stored.	<code>-C {cache file name}</code>
Display the details of the library file.	<code>-v</code>
Update the library file information in the specified location on the command line instead of the default location.	<code>-n /[location]</code>

 The `ld.so.conf` file contains the location details of the shared libraries.

Procedure Reference: Set a Custom Path for Additional Library Files

- To set a custom path for additional library files:
1. Log in as root.

2. To open the profile file, on the terminal, enter `vi /etc/profile`.
3. Specify the location of the other library files and export the library path variable.
 - a. To define the `LD_LIBRARY_PATH` variable, in a new line, enter
`LD_LIBRARY_PATH=/usr/lib:/lib:/Location of the other library files`.



While defining the `LD_LIBRARY_PATH` variable, you must specify the default path of the shared library along with the location of the newly added library files.

- b. To convert the `LD_LIBRARY_PATH` variable to an environment variable, enter `export LD_LIBRARY_PATH`.
4. Save and close the file.
5. Log out and log in as root to update the changes.

DISCOVERY ACTIVITY 7-8

Managing Shared Libraries

Scenario:

Based on a project requirement, a colleague working in the software department wants to know the library files that are needed for an executable program, as well as the process to set a custom path for any additional library file that might be installed.

-
1. Which command will you use to list the shared library files available for an executable program?
 - a) `ld` /[Location of the executable file]
 - b) `ldd` /[Location of the executable file]
 - c) `ldconfig` /[Location of the executable file]
 - d) `lddlibc4` /[Location of the executable file]
-
2. True or False? You have added a few new library files. To update the changes to the `/etc/ld.so.cache` file, you need to run the `ldconfig` command.
☐ True
☐ False
-

LESSON 7

3. **Identify the correct sequence of steps to be followed in specifying a location for the system libraries.**

Save and close the file.

Log out and log in.

Access vi /etc/profile.

Type `LD_LIBRARY_PATH=/usr/lib:/lib:[Location of the other library files]`.

Export the `LD_LIBRARY_PATH` variable.

Lesson 7 Follow-up

In this lesson, you managed packages using package managers and explored the various repositories from where you can download the packages. This will enable you to easily install software packages on Linux systems.

1. **What are the pre-installation steps to be carried out before installing a package?**
2. **Why do you think it is important to create your own repositories?**

LESSON 8

Managing Kernel Services

Lesson Time*1 hour(s), 45 minutes*

In this lesson, you will manage kernel services.

You will:

- Identify the role and functions of the Linux kernel.
- Customize kernel modules.
- Create an initrd image.
- Manage device drivers.
- Monitor the hardware devices available on a computer.
- Monitor processes and resources.

Introduction

In the last lesson, you managed packages to better modify the software running on your Linux system, which might be different depending on the Linux distribution you are using. But there are some aspects of Linux that are consistent, and those are typically handled by the kernel. The kernel, being the core of the Linux operating system, handles various crucial functions such as system initialization, process scheduling, and memory and hardware management. In this lesson, you will explore the role of kernel services and kernel service configuration.

As a Linux system administrator, you may need to configure, modify, and customize the kernel to meet user requirements. Even a minor misconfiguration may cause kernel malfunction, rendering the system ineffective. Therefore, an in-depth knowledge of kernel services is required to manage the kernel efficiently.

This lesson covers all or part of the following CompTIA Linux+ Powered by LPI certification objectives:

- Topic A:
 - Objective 103.1
- Topic B:
 - Objective 101.1, Objective 101.2
- Topic D:
 - Objective 101.1
- Topic E:
 - Objective 101.1
- Topic F:
 - Objective 103.1, Objective 103.5

TOPIC A

Explore the Linux Kernel

The first component that initializes in the Linux boot process is the kernel. It provides all the essential services that are required for running the computer and controls the rest of the processes that operate on the computer. In this topic, you will identify the role of the Linux kernel and its functions.

If a system crashes or stops performing, it actually means that the kernel or an operation critical to the working of the kernel has failed. As a Linux administrator, you need to understand the functionality of the kernel to be able to troubleshoot and provide solutions.

The Kernel

Definition:

The kernel is the core of an operating system. All other components rely on it. It is loaded first and remains in the main memory. It contains system-level commands and other functions that are hidden from users. The kernel manages filesystem access, memory, processes, devices, and resource allocation on a system. The kernel also controls all the hardware devices plugged into the system.

Example:

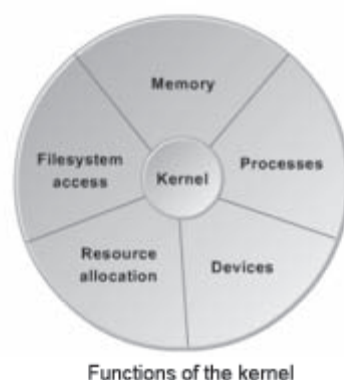


Figure 8-1: The kernel's role in an operating system.

The Linux Kernel

The *Linux kernel*, which is the core constituent of the Linux operating system, manages all other resources on the system. It performs functions such as sharing resources and allocating memory, input and output operations, security settings, and user access. It controls the interaction between software applications and underlying system resources. The kernel initializes itself during the boot process and then starts running the other processes. By default, the kernel loads with a minimal set of functions required to run a system. The kernel's functionality can be expanded by installing kernel modules. The kernel is required to synchronize the operations of multiple processes and govern resources.

Kernel Versions and Modules

Linux kernel versions refer to the different editions of the Linux kernel. Kernel versions are identified by their kernel number, which consists of four parts. The format of the version number is

`major_version_number.major_revision_number.minor_revision_number.fix_number`

The version number can be viewed using the `uname -r` command. Common kernel modules include `input`, `ext3`, `CD-ROM`, `lp`, `udf`, and `jbd`.

Kernel Layers

The kernel performs various functions to control and manage the operations of a system. It is composed of various layers.

Kernel Layer	Function
<i>System Call Interface (SCI)</i>	Handles function calls sent from user applications to the kernel. A function call is basically a service request sent to the operating system's kernel for invoking system-level functions such as requests for processing time and memory allocation. This layer also enables the kernel to schedule and process function calls and manage multiple function calls simultaneously.
<i>Process management</i>	Handles different processes by allocating separate execution space on the processor and ensuring that the running of one process does not interfere with other processes. The kernel implements sharing of the processor time for executing multiple processes through process scheduling.
<i>Memory management</i>	Manages the computer's memory, which is one of the complex tasks performed by the kernel. Like processor sharing, the system's memory also needs to be shared among different application services and resources. The kernel maps or allocates the available memory to applications or programs on request and frees the memory automatically when the execution of the programs are complete, so that it can be allocated to other programs.
<i>Filesystem management</i>	Manages the filesystem, which involves storing, organizing, and tracking files and data on a computer. The kernel also supports a virtual filesystem that provides an abstract view of the underlying data that is organized under complex structures, so that it appears to be a single structure.
<i>Device management</i>	Manages devices by controlling device access and interfacing between user applications and hardware devices of the computer. When the user application sends a system call, the kernel reads the request and passes it on to the drivers that manage the activities of that particular device. For this purpose, the kernel maintains a list of devices in the /dev directory.

Types of Kernels Available in Linux

Kernels can be classified as monolithic or modular.

Kernel Type	Description
<i>Monolithic</i>	In a monolithic kernel, all modules, such as device drivers or filesystems, are built-in. Monolithic kernels can interact faster with devices. But the major disadvantage is its huge size, which leads to higher usage of RAM.
<i>Modular</i>	In a modular kernel, only a minimal set of essential modules are built-in. The rest of the modules can be installed and the kernel can be rebuilt whenever necessary. A modular kernel is also known as a micro kernel or a dynamic kernel. Modular kernels are flexible and save memory usage because the kernel modules, which are loaded as required, are removed from the memory when the related devices are unmounted.

ACTIVITY 8-1

Exploring the Role and Functions of the Linux Kernel

Scenario:

As a system administrator, you may need to troubleshoot issues related to the kernel. So, you want to explore the kernel concepts to refresh your knowledge.

1. Which function is associated with the SCI layer of the kernel?
 - a) Passing requests to device drivers
 - b) Sending service requests to the kernel
 - c) Processor time allocation for functions
 - d) Process scheduling functions
 - e) File organization
2. What are the major functions performed by the kernel? Select all that apply.
 - a) Kernel initialization
 - b) Process management
 - c) Memory management
 - d) Module installation
 - e) Dependency management

3. True or False? The kernel maintains a list of all the devices in the /boot directory.
- ☐ True
- ☐ False

TOPIC B

Customize Kernel Modules

In the previous topic, you familiarized yourself with the basic concepts of the Linux kernel. Kernel modules are functions that extend the capability of the kernel to support additional functionalities. In this topic, you will customize kernel modules.

The Linux kernel, by default, loads with a minimum set of kernel modules. When you want the kernel to support some additional functionality, you have to install or load the necessary modules manually. Customizing the modules to suit user requirements will enable you to manage the kernel efficiently.

Kernel Modules

Definition:

A *kernel module* is a system-level function that extends the functionality of the kernel. It can be dynamically loaded into the kernel or unloaded from the kernel when required. It enables the kernel to update or recompile itself without requiring the system to reboot. The kernel module file consists of a .ko extension. Modules built for a specific kernel version may not be compatible with another version of the kernel.

Example:

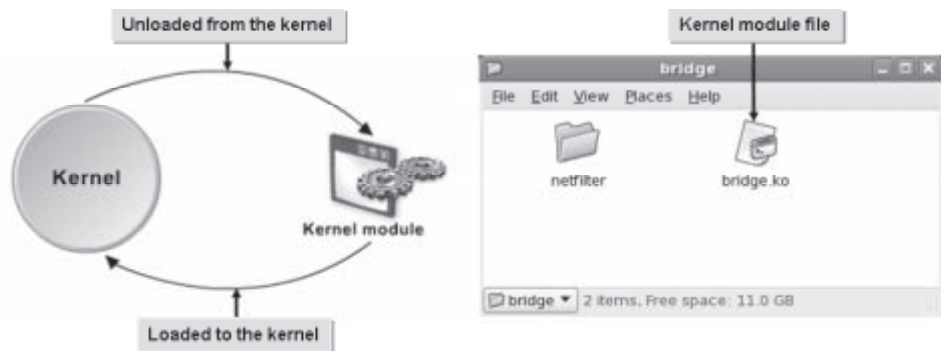


Figure 8-2: *bridge.ko* is the kernel module for network support.

Advantages of Kernel Modules

The advantages of kernel modules are:

- Kernel modules reduce the burden on the kernel. If there are no kernel modules, their functionalities have to be added directly to the kernel image, which can make the kernels larger.
- Kernel modules avoid rebuilding and rebooting of the system when a new functionality is required.
- Dynamic loading of kernel modules facilitate lower memory consumption.

Directories Containing Kernel Modules

The `/lib/modules` directory contains the modules of different kernel versions that are installed. It contains a directory named after the kernel's version number. A list of currently loaded modules is found in the `/proc/modules` file. Modules are stored across various directories based on the categories they belong to. The following table lists the directories containing modules.

Directory	Contains Modules For
<code>pcmcia</code>	PCMCIA (PC Card).
<code>net</code>	Network-related products such as firewalls and protocols.
<code>drivers</code>	Various types of hardware.
<code>fs</code>	Various types of filesystems.
<code>arch</code>	Architecture specific support.

Kernel Module Managing Utilities

A kernel module managing utility enables you to view, load, unload, or modify kernel modules.

Kernel Module Utility	Enables You To
<code>lsmod</code>	Display the currently loaded kernel modules, their sizes, usage details, and their dependent modules.
<code>modinfo</code>	Display information about a particular kernel module such as the file name of the module, license, description, author's name, module version number, dependent modules, and other parameters or attributes. The syntax of this command is <code>modinfo [options]</code> .
<code>insmod</code>	Install a module into the currently running kernel. This utility inserts only the specified module and does not insert any dependent module. The syntax of this command is <code>insmod {file name} [options]</code> .

Kernel Module Utility

Enables You To

modprobe

Add or remove modules from a kernel. This utility is capable of loading all the dependent modules before inserting a specified module.

- The syntax for adding a module is:
`modprobe {module name}`.
- The syntax for removing a module is:
`modprobe -r {module name}`.

Command Options for modinfo

The command options for the `modinfo` command are listed in the table.

Command Option	Enables You To
<code>-V</code>	Display the version number of the <code>modinfo</code> utility.
<code>-n</code>	Display the file name of the module.
<code>-a</code>	Display the author of the module.
<code>-d</code>	Display the description about the module.
<code>-p</code>	Display the parameters supported by the module.

Command Options for insmod

There are several command options for the `insmod` command.

Command Option	Enables You To
<code>-e {persistent name}</code>	Add persistent parameters to the module.
<code>-f</code>	Force the loading of a module even when there is a difference between the module's kernel version and the current kernel version.
<code>-L</code>	Prevent simultaneous loading of the same module.
<code>-o {module name}</code>	Specify a module name while installing the module.

Command Options for modprobe

There are several command options for the `modprobe` command.

Command Option	Enables You To
<code>-a</code>	Add all the modules specified in the command line.

Command Option	Enables You To
-r	Remove all the modules specified in the command line.
-v	Display the verbose of all the commands when they are executed.
-l	List all the modules that match the given wildcard information.
-t {directory name}	List all the modules present in a specified directory.

The modprobe.conf File

The modprobe.conf file is a configuration file, which contains settings that apply persistently to all the modules loaded on the system. It is used to configure modules and their dependencies and also specify module aliases.

 The /etc/modules.conf file was used to manage kernel modules in older versions of Linux.

The modprobe.conf file, which is located in the /etc/modprobe.d directory, has a number of options for configuring kernel modules.

Option	Used To
alias {wildcard} {module name}	Specify an alternate name for a module with a long name.
include {file name}	Add configuration files to a module.
options {module name} {option}	Specify the options to be added to each module before insertion into the kernel.
install {module name} {command}	Run the command specified without inserting the module into the kernel.

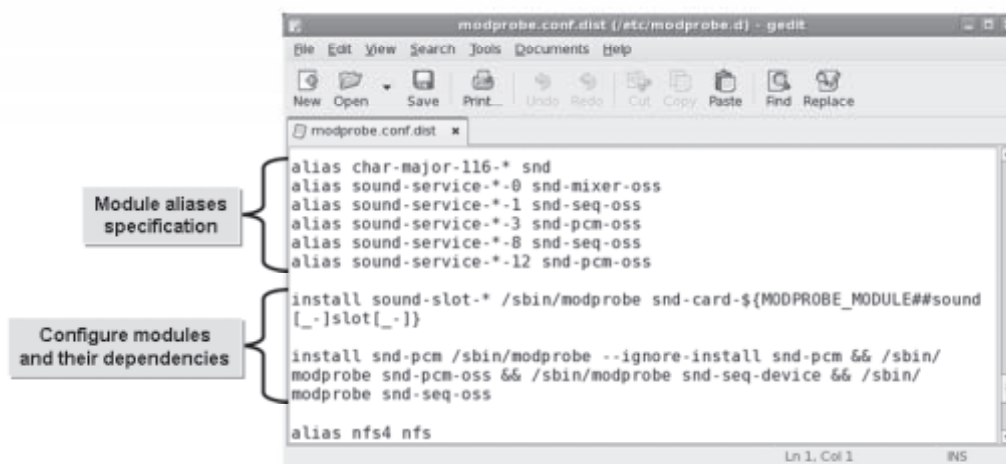


Figure 8-3: The modprobe.conf file is used to configure the kernel modules.

Kernel Options

Kernel options allow you to pass parameters to the kernel at the time of booting a system. These options are used to customize the kernel to suit the individual system or to troubleshoot booting issues. Some of the common kernel options are listed in the following table.

Kernel Option	If You Need To
1 or s	Switch to runlevel 1.
2	Switch to runlevel 2.
3	Switch to runlevel 3.
4	Switch to runlevel 4.
5	Switch to runlevel 5.
rw	Mount the root device in read-write mode while booting the system.
ro	Mount the root device in read-only mode while booting the system.
debug	Enable kernel debugging and log important system events.

Types of Kernel Configuration

Linux kernels can be configured in two different ways.

Kernel Configuration Type	Description
<i>Persistent</i>	Refers to the configuration of kernel settings that do not change even after the system is rebooted. The changes made to the kernel are permanent. The kernel configuration with the <code>sysctl.conf</code> file is persistent and does not get effaced when the kernel is initialized again.
<i>Transactional</i>	Refers to updating the kernel settings for a required service. These settings are not permanent and are reverted when the system is rebooted. The settings hold good only for a particular transaction of the kernel. The kernel configuration with the <code>/proc</code> file is transactional and the changes are reflected immediately. This type of configuration can be used for network services modification and features related to memory subsystems.

The `/proc/version` File

The `/proc/version` file specifies the version of the Linux kernel, the *GNU Compiler Collection* (GCC), and the Linux distribution installed on the system.



Figure 8-4: Details displayed by the `/proc/version` file.

 GCC originally stood for GNU C Compiler because it was produced by the GNU project.

The `/proc` Directory

The `/proc` is a directory in the Linux virtual filesystem, which provides elaborate information about the kernel's running process. Some of the files in the `/proc` directory are listed in the table below.

File	Description
<code>/proc/cmdline</code>	Contains the command line passed to the kernel by the boot loader at boot time.
<code>/proc/cpuinfo</code>	Stores the CPU information and system architecture dependent items.
<code>/proc/devices</code>	Contains the list of device drivers configured into the currently running kernel.
<code>/proc/filesystems</code>	Contains the list of filesystems that are configured into the kernel.
<code>/proc/partitions</code>	Contains partition information including the major and minor number of each partition, partition name, and number of blocks.
<code>/proc/ip_forward</code>	Permits interfaces on the system to forward packets to one other.
<code>/proc/meminfo</code>	Contains memory information such as the used and unused memory on the system and the shared memory and buffers used by the kernel.

The sysctl Command

The *sysctl* command is used to view or set the kernel parameters at runtime. It has various options. Persistent kernel settings are added in the *sysctl.conf* file.

Command Option	Used To
<code>-w {variable}={value}</code>	Set a parameter value or to change the <i>sysctl</i> setting.
<code>{variable}={value}</code>	Set a key parameter value.
<code>-n</code>	Disable the printing of the key name while displaying the kernel parameters.
<code>-e</code>	Ignore errors about unknown keys.
<code>-a</code>	Display all the parameter values that are currently available.
<code>-A</code>	Display all the parameter values that are currently available in a tabular format.

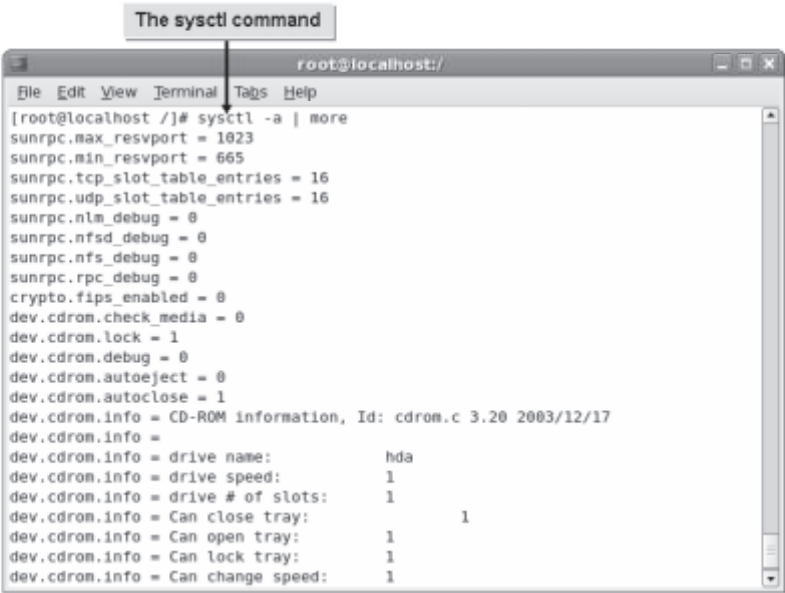


Figure 8-5: The different options of the *sysctl* command.

Syntax

The syntax of the *sysctl* command is *sysctl [options] {kernel parameter}={value}*.

How to Customize Kernel Modules

Procedure Reference: Load Modules Using the insmod Command

To load modules using the *insmod* command:

1. Log in as root in the CLI.
2. To insert a specified module into the kernel, enter *insmod {module name}*.

3. To view detailed information about the inserted module, enter `modinfo [options] {module name}`.

Procedure Reference: View Information About the Running Kernel Modules

To view information about the running kernel modules:

1. Log in as root in the CLI.
2. To view the status of all the loaded modules, enter `lsmod`.

Procedure Reference: Add or Remove Modules Using the modprobe Utility

To load modules using the modprobe utility:

1. Log in as root in the CLI.
2. To add the specified module and all its dependent modules into the kernel, enter `modprobe {module name}`.
3. To view the status of the loaded modules, enter `lsmod`.
4. If necessary, to remove a loaded module, enter `modprobe -r {module name}`.

Procedure Reference: Configure Modules Using the modprobe.conf File

To configure modules using the modprobe.conf file:

1. Log in as root in the CLI.
2. To remove a loaded module, enter `cd /etc`.
3. To open the modprobe.conf file, enter `vi modprobe.conf`.
 - Specify the parameter to pass through when the module is loaded.
 - Set the aliases for a module name.
4. Save and close the file.

Procedure Reference: Manage the Kernel Using the /etc/sysctl.conf File

To manage the kernel using the /etc/sysctl.conf file:

1. Log in as root in the CLI.
2. Open the /etc/sysctl.conf file.
3. Make the necessary modifications to the kernel settings.
4. Save and close the file.
5. Reboot the system.

Procedure Reference: Configure the Kernel Using the /proc Directory

To configure the kernel using the /proc directory:

1. Log in as root in the CLI.
2. To configure the kernel parameters, enter `echo {value} > /proc/{file location whose value in the kernel needs to be changed}`.
3. Save and close the file.

Procedure Reference: Configure the Kernel Using the sysctl Command

- To configure the kernel using the `sysctl` command:
1. Log in as root in the CLI.
 2. To configure the kernel parameters, enter `sysctl [options] {kernel parameter}={value}`.

ACTIVITY 8-2

Inserting and Configuring a Kernel Module

Before You Begin:

1. You have logged in as root in the GUI and the terminal window is displayed.
2. To change to the / directory, enter `cd /`.
3. To unload the kernel module for Bluetooth devices, in the terminal window, enter `modprobe -r bcm203x`.
4. To clear the terminal screen, enter `clear`.
5. Log out root in the GUI.
6. Switch to the first terminal in the CLI.

Scenario:

Your colleague, Mark, tried to transfer some documents from his Linux system to his mobile device. However, he was unsuccessful. After examining the system to try and discover why, you discover that the kernel module required for Bluetooth support is not available.

What You Do	How You Do It
1. Insert the bluetooth kernel module.	<div>a. Log in as root in the CLI.</div> <div>b. To insert the bluetooth module, enter insmod /lib/modules/2.6.18-128.el5/kernel/drivers/bluetooth/bcm203x.ko</div>
2. View information about the inserted bluetooth module.	<div>a. To view information about the bluetooth module, enter modinfo /lib/modules/2.6.18-128.el5/kernel/drivers/bluetooth/bcm203x.ko</div> <div>b. Observe the displayed information about the loaded bluetooth module.</div>

3. Configure the bluetooth kernel module.
 - a. To navigate to the `/etc` directory, at the command prompt, enter `cd /etc`
 - b. To open the `modprobe.conf` file for modification, enter `vi modprobe.conf`
 - c. To go to the last line, press **Shift+G**.
 - d. To switch to insert mode and move to a new line, press **O**.
 - e. To specify an alias name for the bluetooth module, on a new line, type **alias blue bcm203x**
 - f. To switch to command mode, press **Esc**.
 - g. Save and close the file.
 - h. To log out, enter `logout`
-

TOPIC C

Create an initrd Image

In the last topic, you configured and customized kernel modules. The `initrd` image, or the initial ramdisk image, consists of all the kernel modules that were loaded during the boot process. Additional modules that are installed also need to be added to the `initrd` image to load them automatically at boot time. In this topic, you will create the `initrd` image to update the kernel.

The existing kernel on your system may have all the necessary modules, but at a later stage, you may need to update the modules when a new set of devices have to be supported. Knowing how to update the existing modules by creating the `initrd` image will enable you to provide support for new devices.

initrd

initrd refers to the initial ramdisk that is temporarily mounted as the root filesystem for loading startup programs and modules. The ramdisk loads along with the kernel, which controls its functionality. `initrd` enables the system to be started in two phases. In the first phase, the system is booted with the minimal set of modules required to load the main or the permanent root filesystem. In the second phase, when the main root filesystem is mounted, the previously mounted `initrd` filesystem is removed and the ramdisk is released for installing additional modules on demand.

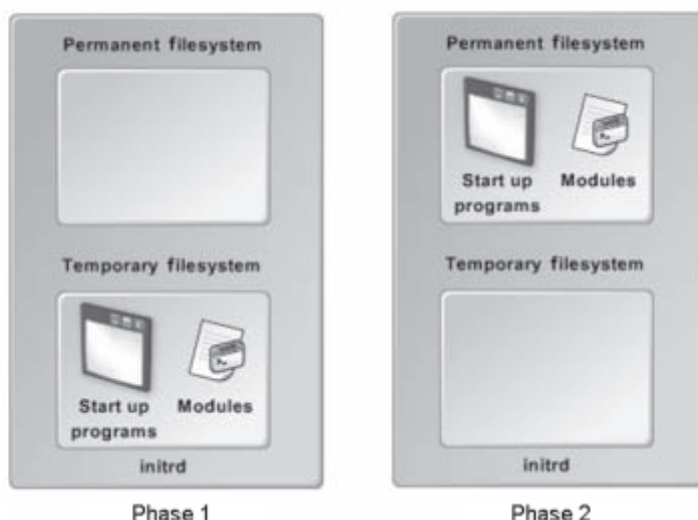


Figure 8-6: The `initrd` starts the system in two phases.

The `initrd` Image

The *initrd image* is an archived file containing all the essential files that are required for booting the operating system. It can be built or customized to include additional modules, remove unnecessary modules, or update existing modules.

The `mkinitrd` Command

The *mkinitrd* command is used to create the initial ramdisk image for preloading the kernel modules.

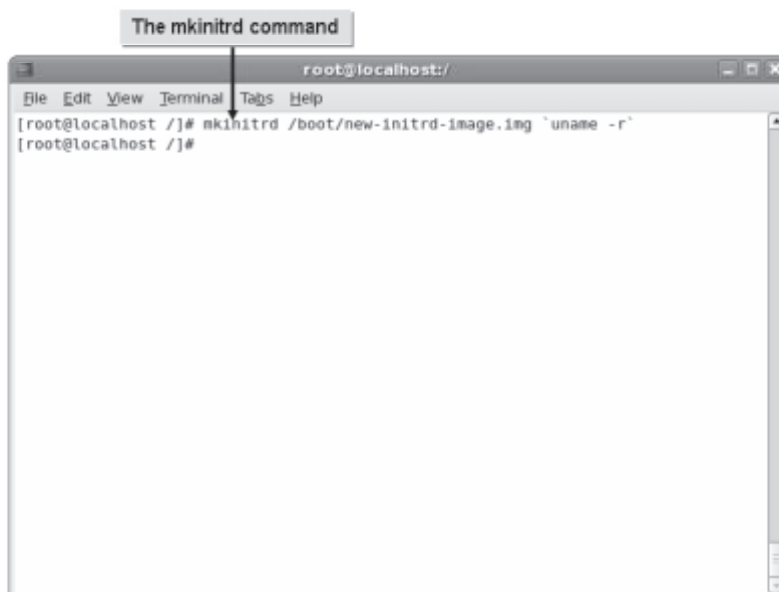


Figure 8-7: New image created using `mkinitrd` command.

Various options of the `mkinitrd` command are given in the following table.

Command Option	Used To
<code>--preload={module name}</code>	Load a module in the initrd image before the loading of SCSI modules.
<code>--with={module name}</code>	Load a module in the initrd image after the loading of SCSI modules.
<code>--fstab={fstab}</code>	Automatically determine the type of filesystem that the root device is found on.
<code>--builtin={module name}</code>	Specify that the module is already built into the currently loaded kernel, so that the <code>mkinitrd</code> command will omit it while creating the initrd image.
<code>--omit-lvm-modules</code>	Avoid loading the LVM modules while creating the initrd image.
<code>--omit-raid-modules</code>	Avoid loading the RAID modules while creating the initrd image.
<code>--omit-scsi-modules</code>	Avoid loading the SCSI modules while creating the initrd image.
<code>-f</code>	Overwrite an existing initrd image file.

How to Create an initrd Image

Procedure Reference: Create an initrd Image with Updated Information

To create an initrd image with updated information:

1. Log in as root in the CLI.
2. To create an initrd image, enter `mkinitrd [options] /boot/initrd-{kernel version number}.img {kernel version number}`.
3. Update the `/boot/grub/grub.conf` file with the updated initrd information.

ACTIVITY 8-3


Creating an initrd Image to Update the Kernel

Before You Begin:

- 1. Reboot srvB and start Red Hat Linux on the system.
- 2. Switch to the first terminal in the CLI.

Scenario:

You have to troubleshoot a Linux system that has a booting issue. The system consists of a SCSI disk containing the Linux installation files. However, the kernel does not have a built-in SCSI module. Though the kernel can load and execute other modules, it will not be able to mount its root filesystem without loading the SCSI module first. Because the module resides in the root filesystem in /lib/modules/, you cannot pre-enable the SCSI support. You have updated the kernel and need to boot the new kernel.

What You Do	How You Do It
1. Create a new initrd image.	<div>a. In the CLI, log in as root.</div> <div>b. To create a new initrd image, enter mkinitrd /boot/new-initrd-image.img 'uname -r'</div> <div> In the 'uname -r' section of the mkinitrd /boot/new-initrd-image.img 'uname -r' command, use the back quote (`) key on the keyboard.</div>

2. Update the GRUB configuration with the new initrd image.
 - a. To access the directory where GRUB is located, enter **cd /boot/grub**
 - b. To edit the GRUB configuration file, enter **vi grub.conf**
 - c. To navigate to the seventeenth line in the file, enter **:17**
 - d. To switch to insert mode, press **I**.
 - e. Verify that the cursor is near the text that starts with "initrd /initrd-2.6.***.img" or "module /initrd-2.6.***.img."
 - f. To display the line as a comment, type **#**
 - g. On a new line, type **module /boot/new-initrd-image.img**
 - h. To switch to command mode, press **Esc**.
 - i. Save and close the file.
 - j. To load the new initrd image, enter **reboot**
-

3. View the new initrd image and boot the system using it.
 - a. When the system reboots and the GRUB splash screen displays the message **Booting Red Hat Enterprise Linux (2.6.****) in 3 seconds**, press **Esc** to enter the boot loader menu.
 - b. If prompted for password, press **P** to view the **Password** prompt. At the prompt, enter your password.
 - c. On the boot loader menu, verify that your currently installed Linux version is selected and press **E** to view its components.
 - d. Observe that the newly created initrd image **module /new-initrd-image.img** is displayed in the boot sequence list.
 - e. Select the new image.
 - f. Press **B** to boot from the new initrd image.
-

TOPIC D

Manage Device Drivers

Throughout this lesson you have been performing various kernel service management tasks. Device management is another important service provided by the kernel. In this topic, you will manage kernel-based device drivers.

A system administrator has to read and write details to the driver files frequently when additional hardware is required or existing hardware is upgraded. Knowing how to access drives through the `/dev` directory will enable you to handle this task effectively.

udev

udev is a device manager that manages the automatic detection and configuration of hardware devices. *udev* is an integral part of the kernel, which is initialized during boot time. The *udev* utility handles module loading for both coldplug and hotplug devices. It loads the modules for coldplug devices, such as a monitor or a sound card, when the system is booted. The modules for hotplug devices, such as a USB drive or a camcorder, are loaded by *udev* dynamically during system run time.

The `/dev` Directory

The `/dev` directory includes hardware and software device drivers.

Coldplug vs. Hotplug

Hotplug is the ability of a system to add or remove hardware without rebooting the system, while coldplug is the inability to do so. Hotplug devices are detected by the system as they are plugged in, whereas coldplug devices, such as conventional hard disks, are not sensed when connected to a running system; they need a complete reboot of the system to function. Some coldplug devices, such as hard disk, PCI, and RAM, can be connected only when the system is not running.

The /sys Directory

In Kernel 2.6 or above, the /sys directory contains information about hotplug hardware devices and displays them in a hierarchical format. It is similar to the /proc filesystem because it contains information related to files loaded in the kernel memory. The sys directory is mounted by default and can be listed using the `mount` command. The sys directory is mounted as a sysfs filesystem, a virtual filesystem.

Device Drivers

Definition:

A *device driver* is a software program that enables a computer's operating system to identify the characteristics and functions of a hardware device, communicate with it, and control its operations. It acts as an interface between the operating system and hardware devices such as hard drives, CD/DVD drives, printers, scanners, monitors, and keyboards. Device drivers can be part of the operating system or installed on demand.

Example:

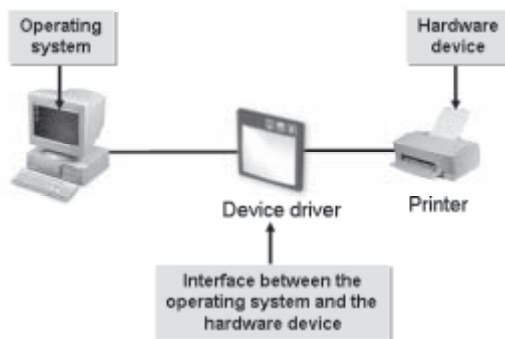


Figure 8-8: A printer driver is used by the operating system to communicate with your printer to print files or documents.

Device Tree

A *device tree* is a structure that lists all hardware devices installed on a system and assigns device nodes to them. It is auto generated by the computer's RAM when the computer is started, when a new device is installed, or when a device or system configuration is modified.

Device Nodes

A *device node* is an access point for device drivers; it is used while mapping service requests with device access. It represents a particular hardware resource in a device tree. It is also known as a device file or a device special file. A node contains vital information such as the device type, the major number, and the minor number. A *minor number* identifies a particular device and the *major number* identifies the device driver that controls this particular device. Device nodes are located in the /dev directory.

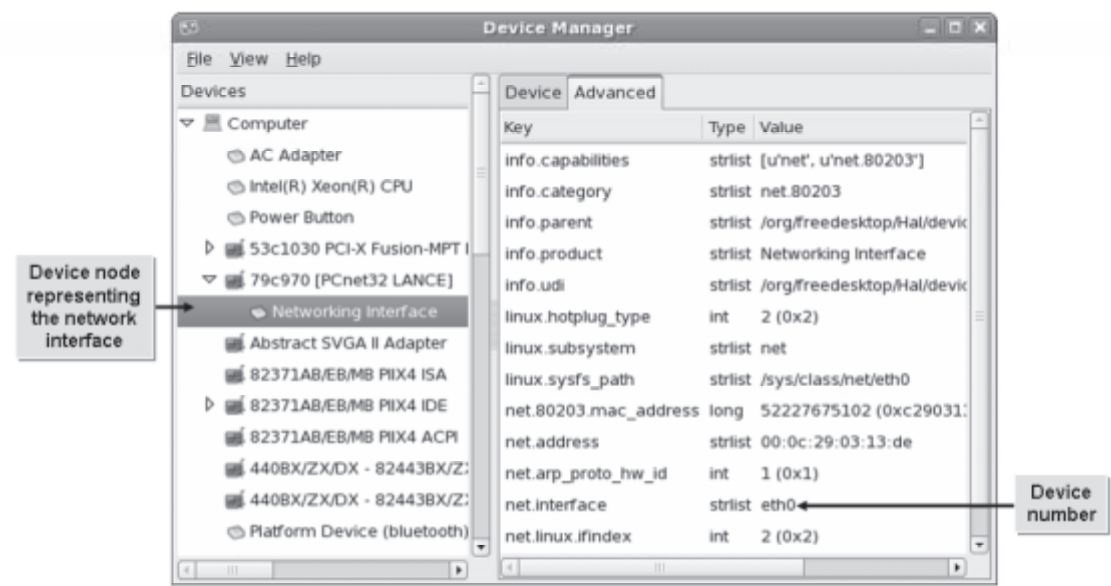


Figure 8-9: A device node representing the disk volume.

Types of Hardware Devices

Hardware devices can be divided into two types based on their usage or function.

Device Type	Description
Block devices	<p>These are typically used for data storage. They buffer all the service requests received to choose the order in which the requests have to be responded. Block devices accept input and provide output in the form of blocks, which are of larger byte sizes. Examples are:</p> <ul style="list-style-type: none">• Hard disks—/dev/hda and /dev/sda• Software RAID—/dev/md[0-5]
Character devices	<p>These are typically used for data streaming and do not use buffering to handle service requests. They accept input and provide output in smaller byte sizes. Examples are:</p> <ul style="list-style-type: none">• Software devices—/dev/null and /dev/zero• Virtual consoles—/dev/tty[0-6]

Special Devices

Linux provides a few special character devices that are used occasionally.

Special Device	Description
/dev/zero	Provides unlimited null characters (0 bytes) for writing into any program or file. It is used for generating an empty file of certain size.
/dev/null	Does not provide any data to a program or file. It discards all data written to it. It is used as an output file when the output is not required by the user.
/dev/random	Functions as a random number generator. It gathers random input from device drivers and other sources on the system and saves it as bits in an <i>entropy</i> pool. It provides randomly generated output as bytes to applications within the number of bits in the pool. When the pool is exhausted, the /dev/random device will block the reading application until more random input is collected.
/dev/urandom	Functions similarly to /dev/random, except that it does not block the reading application if the entropy pool is exhausted. It uses a software algorithm to generate alternate random input that may be less secure than the input generated by the system.

The mknod Command

The *mknod* command allows you to create device files that are not present, using the major and minor node numbers of a device.

Syntax

The syntax of the *mknod* command is `mknod [OPTION] {NAME} {TYPE} [MAJOR MINOR]`.

How to Manage Device Drivers

Procedure Reference: Access Drivers Through /dev

To access device driver files through /dev:

1. Log in as root in the CLI.
2. To check which terminal is used and the users who are logged in, enter `who`.
3. To view the device driver file, enter `cat /dev/{device node}`.
4. To send messages using the specific device node, enter `echo {messages} > /dev/{device node}`.

Procedure Reference: Add Files Under /dev

- To add files under /dev:
1. Log in as root in the CLI.
 2. Add files under the /dev directory.
 - Create files in the /etc/udev/rules.d directory.
 - a. To open the rules.d directory, enter `cd /etc/udev/rules.d`.
 - b. To view the timestamps of the device file, enter `touch {file name}`.
 - c. Switch to insert mode.
 - d. To open the device file, enter `vi {file name}`.
 - e. To add details to the file, type the text as indicated below.`KERNEL=="{device}", NAME="{device node}"`.
 - f. Save and close the file.
 - Create files using the `mknod` command.
 - a. To create the device node, enter `mknod /dev/{device node} {device type} {major number} {minor number}`.

ACTIVITY 8-4

Accessing Drivers Through /dev

Before You Begin:
On srvA, switch to the GUI.

Scenario:
Your company has a server to which many users log in with their user account to carry out some day-to-day tasks. Due to unscheduled emergency maintenance on the server, you may need to reboot the system. You now need to send a message to all the currently logged in users using the device node, so that they can save their data, complete their tasks, and log out of their systems.

What You Do	How You Do It
1. View information about users who have currently logged in.	<ol style="list-style-type: none">a. Log in as root in the GUI.b. To open the terminal, choose Applications→Accessories→Terminal.c. To check who is logged in to which terminal, enter whod. Observe the list of current users displayed as the output.

2. Send messages using the device node in the `/dev` directory.
 - a. To alert all the current users using the specified device node, enter `echo "Please save your work, the system will be down for maintenance in 30 minutes" > /dev/tty1`
 - b. To clear the terminal window, enter `clear`
 - c. Switch to the CLI.
 - d. Observe that the echoed message is displayed on the screen. To return to the login prompt, press **Enter**.

TOPIC E

Monitor Hardware Devices

Previously, you accessed driver files and modified their parameters. Drivers are associated directly with the hardware devices that are installed on your computer. In this topic, you will monitor various hardware devices.

A system administrator needs to track all the devices that are connected to a computer and monitor them continuously. Gaining knowledge about utilities that are used to track these hardware devices is essential for proper management of a Linux system.

Hardware Communication Channels

The kernel and hardware devices communicate using major channels such as Interrupt Requests, Input/Output (I/O) addresses, and Direct Memory Address (DMA).

Hardware Communication Channel	Description
<i>Interrupt ReQuests (IRQ)</i>	An interrupt request is a signal sent by a hardware device to the kernel to request processing time in order to perform an operation. This enables the kernel to prioritize system events and allocate the CPU's processing time for devices.
<i>Input/Output (I/O) Addresses</i>	Every hardware device communicates with the operating system through a unique I/O address. The kernel uses this address to identify the requests sent to or from the device. It is also used to map the device with user applications requesting the device services.

Hardware Communication Channel	Description
<i>Direct Memory Address (DMA)</i>	A method by which hardware devices directly communicate with the memory to obtain memory allocation without going through the processor.

The HAL

The *Hardware Abstraction Layer (HAL)* is a logical interface that enables software applications to interact with hardware devices at an abstract level through system calls. This layer converts generic system calls sent by software applications to detailed device-specific instructions. It enables an operating system to adapt to different kinds of hardware platforms without requiring any modification in the kernel.

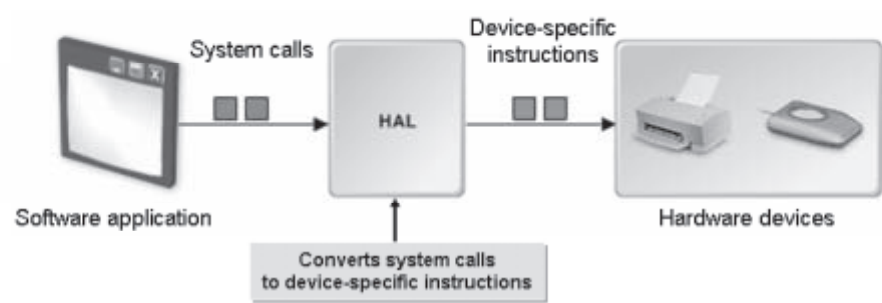


Figure 8-10: HAL serves as an interface between software and hardware.

HAL Utilities

The HAL utilities enable you to view or monitor the hardware device connected to the computer.

HAL Utility	Used To
<code>lspci</code>	Display information about all the PCI buses and all the peripheral components connected to a computer.
<code>lsusb</code>	Display all the USB components connected to a computer.
<code>hal-device</code>	Display the list of all the connected devices in text mode. You can use the options to add or remove devices from the list.
<code>hal-device-manager</code>	Display all the connected devices in a graphical window. This utility is dependent on the <code>udev</code> command for device node information.

The hald Daemon Service

`hald` is a daemon service that contains the list of devices actually connected to the system. `hald` enables the other applications to access or view the devices list by passing information through the Dbus interface.

The Dbus System Bus

Dbus is the system bus that provides the main communication between applications. This contains a daemon that can invoke specific services on the system based on the needs of the requesting application. This daemon can send system wide alerts such as “new hardware detected” and “print queue modified.”

How to Monitor Hardware Devices

Procedure Reference: Monitor Hardware Devices

To monitor the hardware devices currently connected to a system:

1. Log in as root.
2. Monitor hardware devices.
 - To list the status of all PCI devices, enter `lspci`.
 - To list the status all USB devices, enter `lsusb`.
 - To list all devices, enter `hal-device`.
 - To display the Device Manager window and view the list of all hardware devices and their related information, enter `hal-device-manager` or choose **System→Administration→Hardware**.

ACTIVITY 8-5

Monitoring Hardware Devices on a Computer

Before You Begin:

1. Switch to the GUI.
2. You have logged in as root in the GUI.
3. The terminal window is displayed.
4. To navigate to the `/rhelsource/Server` directory, in the terminal window, enter `cd /rhelsource/Server`.
5. To install the HAL device manager package, enter `rpm -ivh hal-gnome-0.5.8.1-38.el5.i386.rpm`.
6. To clear the terminal window, enter `clear`.

Scenario:

As part of your routine system administration tasks, you have to track the devices used on all the computers on the network and maintain a list of hardware resources that are in use.

LESSON 8

What You Do	How You Do It
1. View all peripheral devices that are connected to the system.	<ol style="list-style-type: none">To view the list of peripheral components and their related information, in the terminal window, enter lspci -vObserve the list of hardware devices displayed along with the related information.To clear the terminal window, enter clear
2. View all hardware devices that are connected to the system using the HAL device manager.	<ol style="list-style-type: none">To view the list of all the hardware devices and their related information, enter hal-device-managerObserve that the Device Manager window lists all the hardware devices connected to the system in the left pane.To view more information, in the right pane, select the Advanced tab.Observe that the details are listed under the Key column. Also observe that the active status of the horizontal scroll bar indicates that there are more columns on the right side.To view the Type and Value columns, scroll to the right.Close the Device Manager window.To clear the terminal window, enter clear

TOPIC F

Monitor Processes and Resources

In the last topic, you monitored the hardware devices on your computer. Along with hardware devices, software applications and programs work in conjunction to make the entire system work. Software programs are handled by the processor. In this topic, you will monitor processes to view how system resources are utilized and how the processor manages them.

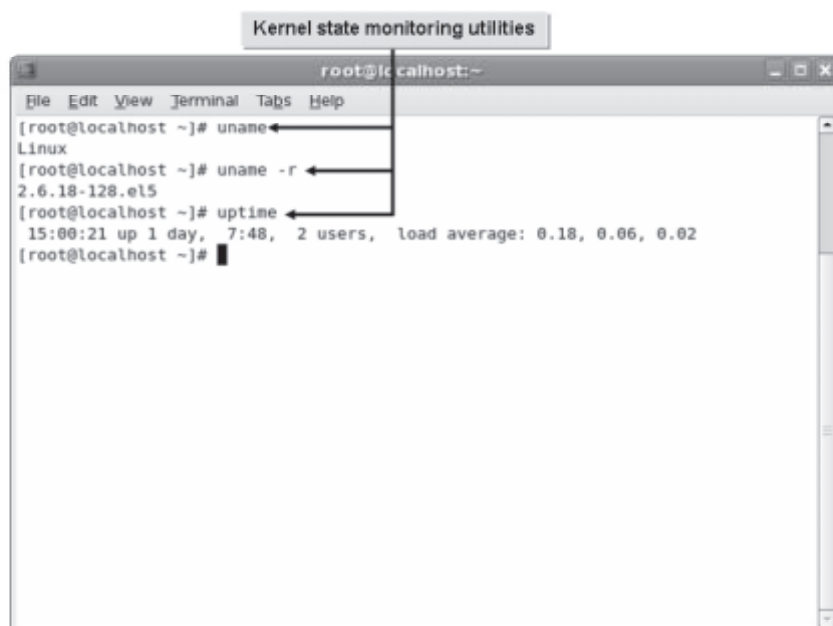
As a system administrator, you may need to handle a number of running processes simultaneously. Based on the need, one program may require a higher priority than another. While the execution of one process is in progress, you may decide to pause or stop the process to start another important process. Performing process monitoring will help you manage multiple programs and their resource allocation.

Load Average

Load average is the average number of processes waiting to run on a system for the last 1 minute, 5 minutes, and 15 minutes. Ideally, the number should be less than one. This information can be used to check whether the system is busy. The load average information is specific to the operating system and the hardware.

Kernel State Monitoring Utilities

Kernel state monitoring utilities are used to gather information about the operating system and its running events and processes. The kernel state monitoring utilities are listed in the table.



```
Kernel state monitoring utilities
root@localhost:~
File Edit View Terminal Tabs Help
[root@localhost ~]# uname
Linux
[root@localhost ~]# uname -r
2.6.18-128.el5
[root@localhost ~]# uptime
15:00:21 up 1 day, 7:48, 2 users, load average: 0.18, 0.06, 0.02
[root@localhost ~]#
```

Figure 8-11: Output of various kernel state monitoring tools.

Kernel State Monitoring Utility	Enables You To
uname	Display the name of the operating system, its version, license, processor, and hardware details.
uptime	Display the duration for which the system has been running, the number of users logged on currently, and the load average of the system.
tlload	Provide a graphical representation of the system and the load average for the past 1 minute, 5 minutes, and 15 minutes.

System Load

System load is a measurement of the amount of work done by a computer over a given period of time. It is represented in the form of three numbers. The first number indicates the system load during the last 1 minute, the second number indicates the system load during the last 5 minutes, and the last number indicates the system load during the last 15 minutes.

Memory Monitoring Utilities

Memory monitoring utilities are used to view the usage of memory and other related statistics.

Memory Monitoring Utility	Enables You To
free	Display the total memory available on the system and the amount of memory that is free, used, shared, buffered, and cached.
vmstat	Display the statistics about virtual memory usage. It lists the details about currently running processes such as memory usage, interrupts or I/O address information, and processor allocation information.
pmap	Display the mapping of processes with memory resources.
iostat	Generate reports on CPU and device utilization. It provides input and output statistics for storage devices and partitions.

Command Options for the free Utility

There are several command options for the `free` utility.

Command Option	Used To
-b	Display the amount of memory in bytes, kilobytes, megabytes, and gigabytes, respectively.
-k	
-m	
-g	
-s <i>{delay in seconds}</i>	Update the memory statistics at a delay of the specified seconds.
-o	Disable the display of the buffer or cache information line.
-t	Display the total RAM and swap space.

Command Options for the vmstat Utility

The command options for the `vmstat` utility are listed in the table.

Command Option	Used To
-a	Display the active or inactive memory.
-s	Display memory statistics in a table format.
-m	Display statistics in the form of slabs.
-d	Display disk statistics.
-p <i>{disk partition}</i>	Display statistics for the specified partition.

Command Options for the pmap Utility

There are several command options for the `pmap` utility.

Command Option	Used To
-x <i>{PID}</i>	Report the memory map of processes in an extended format.
-d <i>{PID}</i>	Report the memory map of processes in a device format.
-q <i>{PID}</i>	Report the minimal required information of memory mapping.
-V	Display the version of the <code>pmap</code> utility.



PID (Process ID) is a unique number assigned by the operating system to each process started on the system.

Process Monitoring

Process monitoring is a mode of tracking the processes running on a system, to determine its performance and reliability. Some processes that run continuously on a system, such as those initiated by databases and web servers, have to be monitored constantly, whereas others can be monitored occasionally. Process monitoring enables a user to identify the causes of low performance in processes and detect the processes run by unauthorized users.

Process monitoring can be performed with the help of various utilities.

Utility	Enables You To
top	Display the list of processes in the descending order of CPU memory usage. It also displays details about the consumption of power, memory, and system resources at a given time. It helps track processes that consume high memory and system resources. The output of the command can also be redirected to a text file. In the KDE desktop environment, the <code>kpm</code> utility is used in place of the <code>top</code> command.
GNOME system monitor	Monitor system performance. It has three tabs, which list the performance history and status of various processes, resources, and filesystems on the system.
sar	Display the system utilization reports that are generated based on the system utilization data. These reports consist of various sections each of which consists of the type of data and the time at which the data was collected. By default, the <code>sar</code> reports list the data collected every 10 minutes. On an average, the report consists of 17 sections. The <code>sar</code> command is run automatically by a script called <code>sa2</code> at specified time intervals.

 The `ps` command allows you to view the running processes on a system.

sar Options

The `sar` command can be used to retrieve specific data by specifying the following options.

Some of the frequently used options are listed in the table.

Option	Enables You To
-A	Display all reports generated on the current date.
-b	Display I/O statistics.
-B	Display the number of bytes paged in between the system and the disk.
-c	Display the number of processes spawned per second by the system.
-d	Display system activity for each block device.

The GNOME System Monitor

The *GNOME system monitor* is a GUI utility that is used to monitor system processes, resources, and filesystems. The **Processes** tab displays details about the currently running processes such as the name, status, ID, and CPU and memory usage. The **Resources** tab displays the history of CPU, memory, and swap usage and network operations. The **File Systems** tab displays information about currently mounted filesystems, related directories, type, and usage status.

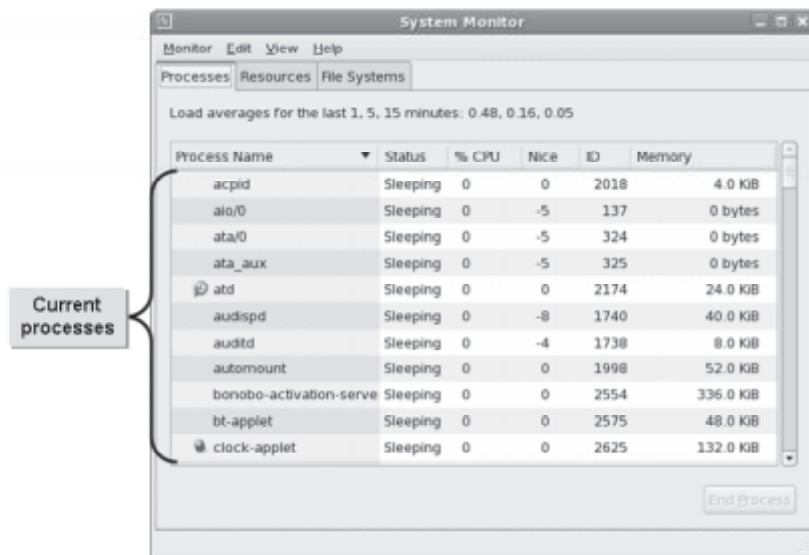


Figure 8-12: The GNOME system monitor displaying the system status.

How to Monitor Processes and Resources

Procedure Reference: Monitor the Kernel State

To monitor the kernel state:

1. Log in as root.
2. To view the information regarding the running kernel, on the terminal, enter `uname [options]`.
3. To view the running time of the system, enter `uptime`.
4. To view the graphical representation of the systems load average in the CLI, enter `load`.

Procedure Reference: Monitor the Memory Usage

To monitor the memory usage:

1. Log in as root.
2. To view the free and used memory of the system, on the terminal, enter `free [options]`.
3. To report the virtual memory statistics, enter `vmstat [options]`.

Procedure Reference: Monitor the Processes Mapping

To monitor the processes mapping:

- 1. Log in as root.
- 2. To view the running processes on the system, enter `ps [options]`.
- 3. To view the memory map of a process, enter `pmap [options] {pid}`.

Procedure Reference: Manage Processes Using the GNOME System Monitor

To manage processes using the GNOME system monitor:

- 1. Log in as root in the GUI.
- 2. To open the GNOME system monitor, choose **System**→**Administration**→**System Monitor**.
- 3. On the **Processes** tab, scroll to locate the process.
- 4. To start, stop, kill, or change priority, right-click on a running process.
- 5. To close the window, choose **Monitor**→**Quit**.

ACTIVITY 8-6

Monitoring Processes and Resources

Before You Begin:


You have logged in as root in the GUI. The terminal window is displayed.

Scenario:

Your company has recently expanded and a large number of users have joined your network. Therefore, there are many services running simultaneously on the main server. To reduce the load on the server, your company wants to add separate servers. As a system administrator, you are asked to submit data on the usage of the existing server to decide on the number of servers to be added and the applications that are to be moved to the additional servers.

What You Do	How You Do It
1. Monitor the kernel state.	<ul style="list-style-type: none">a. To view information related to the release version of the kernel, enter uname -rb. Observe that the kernel version "2.6.18-128.el5" is displayed. To view the running time of the system, enter uptimec. Observe that information about the system start time, the duration, the number of currently logged in users, and the load averages is displayed.

2. Monitor memory usage.
 - a. To view the virtual memory statistics, enter **vmstat**
 - b. Observe that the details are displayed for the processes, memory, swap, input/output, system, and CPU. To view the unused memory available on the system, enter **free -m**
 - c. Observe that the details about memory and swap usage are displayed in the output.
-
3. Monitor processes.
 - a. To view the processes that are currently running on the system, enter **ps aux | more**
 - b. Observe that a list of all the processes with details regarding users who are running the processes, the process IDs, CPU and memory usage, virtual and resident set size, the terminal type, time, and the command is displayed. To return to the prompt, press **Q**.

 VSZ and RSS are the virtual set size and resident set size attributes of a process that display how much memory has been occupied by a process.
 - c. To clear the terminal window, enter **clear**
-

Lesson 8 Follow-up

In this lesson, you explored the purpose and organization of the kernel and managed its services. This will enable you to understand the kernel structure, monitor the kernel components, and configure the kernel services. As a Linux system administrator, customizing the kernel to suit your requirements will enable you to manage the kernel efficiently.

1. How do you think modules affect the way kernels are loaded?

LESSON 8

2. Why is process management important for operating systems?

LESSON 9

Working with the Bash Shell and Shell Scripts

Lesson Time

2 hour(s)

In this lesson, you will work with the Bash shell.

You will:

- Perform basic Bash shell operations.
- Write a basic shell script.
- Use shell variables.
- Redirect standard input and output.
- Use control statements.

Introduction

In the previous lesson, you managed Linux kernel services. In addition to kernel, the Linux shell is an important constituent of the operating system, and it is essential to familiarize yourself with the Bash shell and perform basic operations in it. In this lesson, you will work with the Bash shell and write shell scripts.

The Bash shell functions as an intermediary layer between a user and the operating system. You can use shell scripts within the Bash shell to automate routine administrative tasks.

Although Bash is not the only shell available, it is one of the most common ones, and so familiarizing yourself with the Bash shell and its functions enables you to interact and work efficiently with the Linux operating system.

This lesson covers all or part of the following CompTIA Linux+ Powered by LPI certification objectives:

- Topic A:
 - Objective 103.1, Objective 103.3
- Topic B:
 - Objective 103.1, Objective 105.2
- Topic C:
 - Objective 103.1, Objective 105.1, Objective 105.2, Objective 109.3
- Topic D:
 - Objective 103.4, Objective 105.1, Objective 105.2
- Topic E:
 - Objective 105.1, Objective 105.2

TOPIC A

Perform Basic Bash Shell Operations

In the previous lesson, you familiarized yourself with the working of the shell application and its various types. You are now ready to run commands in the shell to perform basic file navigation in the operating system. In this topic, you will perform basic Bash shell operations.

The Bash shell is the most frequently used shell in Linux. It allows you to effectively perform tasks, such as file management, user and group administration, process management, text editing, and so on, using the command line. Basic Bash shell options allow you to perform simple tasks such as using strings to search for files on your system, reviewing commands that have been previously executed, and many more.

The Bash Shell

The *Bourne-Again SHell* (*Bash shell*) is the default shell in Linux. It is a superset of the Bourne shell and includes features from the Korn and C shells. The Bash shell facilitates command line editing, command history, command line completion, and shell scripting.

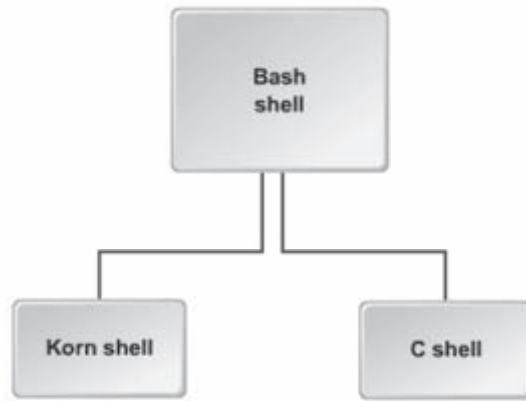


Figure 9-1: *The Bash shell includes features from the Korn and C shells.*

Bash Shell Functions

The shell is the basic component that provides the CLI in Linux. Some of the functions performed by the shell include:

- Prompting a user for input and waiting for a command to be entered.
- Verifying the correctness of the command and processing the command.
- Expanding wildcards by replacing special characters with portions of the string.
- Determining the source of input and the location of output.
- And, returning to the prompt after the completion of a command and restarting the cycle.

Wildcards

Wildcards are special characters that are used to substitute portions of a string. By using wildcards with appropriate arguments, you can search and locate files on your system. Wildcards are used to narrow down search criteria and obtain accurate search results.

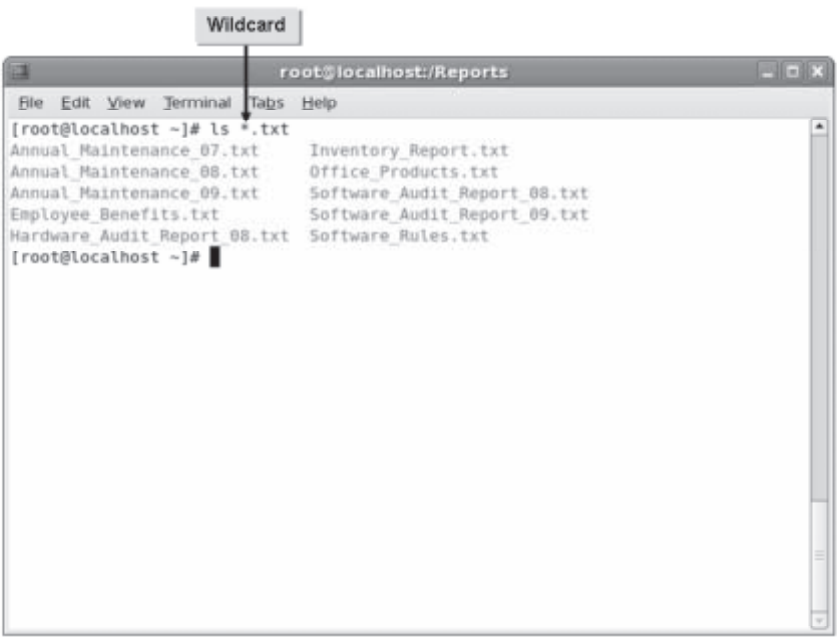


Figure 9-2: Using wildcards in a command.

The following table lists some of the frequently used wildcards.

Wildcard	Used To
*	Match zero or more characters in the file name.
?	Match a single character in the file name.
[abcde]	Match any of the listed characters.
[a-e]	Match any character in the range.
[!abcde]	Match any character that is not listed.
[!a-e]	Match any character that is not included in the range.
{linux, shell}	Match any word in the given options.
\$	List file names that end with the character preceding the \$ symbol.

Complex Wildcards

A complex wildcard is a combination of individual wildcards. For example, enter `[a-z]?[1-9]` to search for three characters—the first character is a letter, the last character a number, and the middle character can be a letter, a number, or a special character.

Globbering


Globbering is a function that expands file names (wildcards) using a pattern-matching behavior. The wildcards that globbering interprets are the asterisk (`*`), the question mark (`?`), sets of characters that are included within brackets, and special characters such as the caret (`^`).

Tab Completion

Tab completion facilitates auto completion of commands and file names. Pressing **Tab** completes the names of commands, files, directories, users, and hosts.



Figure 9-3: Tab completion entries for the text "his".

 Pressing **Tab** two times displays all files and directories that begin with the string you typed.

The history Command

The *history* command is used to view previously typed commands. It retrieves the specified number of commands from the `~/.bash_history` file. You can use the **Up Arrow** or **Down Arrow** key to select the desired command. By simultaneously pressing **Alt** and **Period (.)**, you can recall arguments that have been used with previously executed commands.

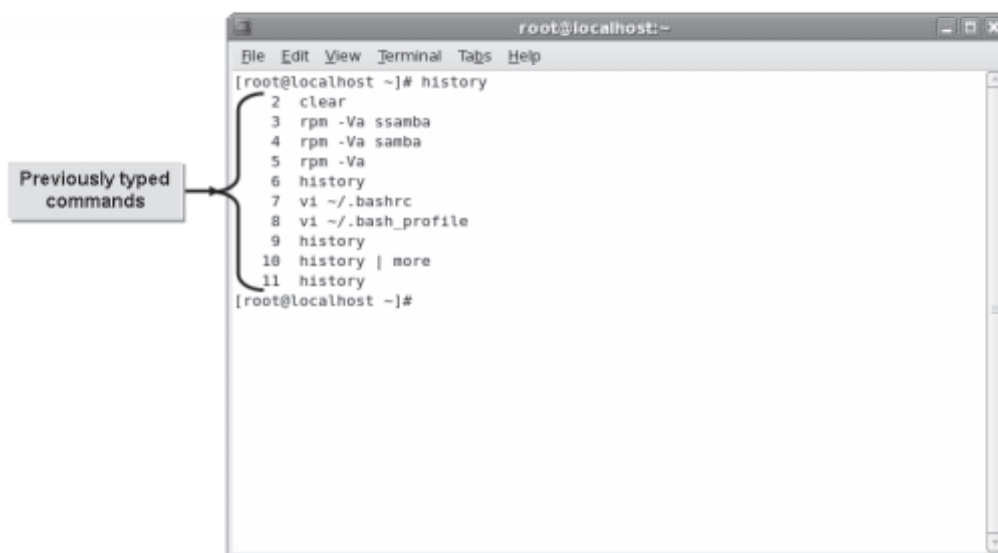


Figure 9-4: Output of the history command.

Recall Commands and Arguments

Pressing the **Up Arrow** key allows you to recall commands that have been run on the terminal. Pressing **Esc** followed by **Period (.)** is an alternate way of recalling arguments.

How to Perform Basic Bash Shell Operations

Procedure Reference: Perform a Search Using Wildcards

To perform a search using wildcards:

1. Log in as a user in the CLI.
2. Perform basic operations.
 - To list all the content that match the given pattern, enter `ls [wildcard]{string}[wildcard]`.
 - To remove all the content that matches the given pattern, enter `rm [wildcard]{string}[wildcard]`.
 - To print all the content that match the given pattern, enter `echo [wildcard]{string}[wildcard]`.

Procedure Reference: Search for Files Using Wildcards

To search for files using wildcards:

1. Log in as root in the CLI and navigate to the relevant directory.
2. Locate the desired files using wildcards.
 - To view all files starting with the search string, enter `find -iname '[search string]*'`.
 - To view all files ending with the search string, enter `find -iname '*[search string]'`.
 - To view all files containing the search string, enter `find -iname '*[search string]*'`.
 - To do a more specific search, enter `find -iname '[complex wildcard][search string]'`.

Procedure Reference: Move Files that Meet a Wildcard Pattern

To move files that meet a wildcard pattern:

1. Log in and navigate to the relevant directory.
2. To move files that meet the search pattern to the target directory, enter `mv *[search string] /{target directory}`.
3. If necessary, to verify that the files have been moved to the target directory, enter `ls /{target directory}`.

Procedure Reference: Detect a File Name Using Tab Completion

To detect a file name using tab completion:

1. Log in as a user in the CLI.
2. To complete the command name, enter a unique character of the command name and press **Tab**.

3. To complete the file name, enter a unique character of the file name and press **Tab**.

Procedure Reference: View the Recently Used Commands Using the history Command

To view the recently used commands using the `history` command:

1. Log in as a user in the CLI.
2. View the history of commands executed.
 - To list all the previously used commands, enter `history`.
 - To execute a particular command from the command history, enter `!{history number}`.
 - To repeat the previously executed command, enter `!!`.

Procedure Reference: Perform Basic Command Line Expansion

To perform basic command line expansion:

1. Log in as a user in the CLI.
2. Perform basic command line expansion.
 - Enter `{command} {common string}{unique part of file 1, unique part of file 2}` when a file or directory name has a common string in it.
 - To print a string, enter `{command} '{string}'`.
 - To send the output of one command as the input to another command, enter `{command 2} '{command 1}'`.

ACTIVITY 9-1

Using Wildcards to Search for Files

Data Files:

- Audit_File_2000.txt
- Audit_File_2001.txt
- Audit_File_2002.txt
- Audit_File_2003.txt
- Audit_File_2004.txt
- Audit_File_2005.txt
- Audit_File_2006.txt
- Audit_File_2007.txt
- Audit_File_2008.txt
- Audit_File_2009.txt
- Audit_File_2010.txt

Before You Begin:

- 1. You have logged in as root in the GUI.
- 2. The terminal window is displayed.
- 3. In the terminal window, enter
`cp /085099Data/Working_with_Bash_and_Shell_scripts/* /root.`
- 4. To overwrite the Software_List.txt file, enter `y`.
- 5. To overwrite the Software_Rules.txt file, enter `y`.
- 6. To change to the root directory, enter `cd /root.`
- 7. To clear the terminal window, enter `clear`.
- 8. Switch to the CLI.
- 9. Log in to the system as root.

Scenario:

You have to create a report on audit file maintenance in your department. You want to generate a list of all the audit files created since the inception of the company, along with the date and time of creation or last modification, ownership details, and file access permissions. Therefore, you decide to use wildcards to search for the audit files in your Linux system.

What You Do	How You Do It
1. Search for the audit files using wildcards.	<ul style="list-style-type: none">a. To list all files that match the search pattern "Audit*", enter <code>ls -l Audit*</code>b. Observe that the resultant files are displayed along with the date and time of creation or last modification, ownership details, and file permissions.
2. Display all file names using wildcards.	<ul style="list-style-type: none">a. To display all file names that match the search pattern "Audit*", enter <code>echo Audit*</code>b. Observe the file names that are displayed.c. Clear the terminal screen.

ACTIVITY 9-2

Viewing the Command History

Before You Begin:

1. You have logged in as root in the first terminal of the CLI.
2. Enter `logout` to log out of the root user account.

Scenario:

While you were on vacation, your colleague, Joyce Smith, had been performing some of your tasks using your system and login name. Now that you are back, you want to view the commands she executed, to create a log of the tasks executed on your system.

What You Do	How You Do It
1. View the command history.	<ol style="list-style-type: none"> a. Log in as jsmith. b. To use the tab completion feature, type hist and press Tab. c. Observe that the full name of the history command is automatically completed. To view the command history, press Enter. d. Observe the last few commands that have been executed on your system. Log out of the jsmith user account.
2. View the command history of the root user.	<ol style="list-style-type: none"> a. Log in as root in the CLI. b. To view the history command, at the command line, type hist and press Tab. c. Observe that the full name of the history command is automatically completed. To view the command history, press Enter. d. Observe the last few commands executed by the root user. Clear the terminal screen.

ACTIVITY 9-3

Organizing Files Using Wildcards

Data Files:

- Software_Audit_Report_2007.txt
- Software_Audit_Report_2008.txt
- Hardware_Audit_Report_2007.txt
- Hardware_Audit_Report_2008.txt
- Annual_Maintenance_Report_2008.txt
- Annual_Maintenance_Report_2007.txt
- New_Policies_2008.txt
- Audit_File_2008.txt
- Audit_File_2009.txt
- Audit_File_2010.txt

Before You Begin:

1. You have logged in as root in the CLI.
2. The first terminal is displayed.

Scenario:

Your organization adopted a new system audit policy that requires you to organize your files in a proper directory structure and make a backup of the directory. You have been asked to create the necessary directory structure and relocate the files to ensure that the structure complies with your organization’s standards.

The files that need to be organized are located in the /root directory.

What You Do	How You Do It
1. Create a directory structure with Audit_Reports as the parent directory, containing four subdirectories named 2007, 2008, 2009, and 2010.	<div>a. To create the Audit_Reports directory, enter mkdir Audit_Reports</div> <div>b. To switch to the newly created directory, enter cd Audit_Reports</div> <div>c. To create multiple directories, enter mkdir 2007 2008 2009 2010</div> <div>d. To list the directories, enter ls</div> <div>e. Observe that the newly created directories are listed.</div>

2. Move the files related to the years 2007, 2008, 2009, and 2010 to their respective directories.
 - a. To switch to the parent directory, enter `cd ..`
 - b. To move the files with names that end with "2007" to the `Audit_Reports/2007` directory, enter `mv *2007.txt Audit_Reports/2007`
 - c. To verify that the files have been moved, enter `ls Audit_Reports/2007`
 - d. Observe that the files are listed, indicating that they have been moved.
 - e. To move the files with names that end with "2008" to the `Audit_Reports/2008` directory, enter `mv *2008.txt Audit_Reports/2008`
 - f. To verify that the files have been moved, enter `ls Audit_Reports/2008`
 - g. Observe that the files are listed, indicating that they have been moved.
 - h. To move the files with names that end with "2009" to the `Audit_Reports/2009` directory, enter `mv *2009.txt Audit_Reports/2009`
 - i. To verify that the files have been moved, enter `ls Audit_Reports/2009`
 - j. To move the files with names that end with "2010" to the `Audit_Reports/2010` directory, enter `mv *2010.txt Audit_Reports/2010`
 - k. To verify that the files have been moved, enter `ls Audit_Reports/2010`
 - l. Observe that the files are listed, indicating that they have been moved. Clear the terminal screen.
-

3. Create a backup for the Audit_Reports directory in a different location.
 - a. To recursively copy all files from the Audit_Reports directory to the /Reports_Backup directory, enter **cp -R Audit_Reports /Reports_Backup**
 - b. To verify that the backup directory has been created, enter **ls /**
 - c. Observe that the backup has been created.

 4. Rename the Reports_Backup directory as Audit_Backup.
 - a. To switch to the parent directory, enter **cd ..**
 - b. To rename the Reports_Backup directory as Audit_Backup, enter **mv Reports_Backup Audit_Backup**
 - c. To verify that the directory has been renamed, enter **ls**
 - d. Observe that the backup directory has been renamed.
 - e. Clear the terminal screen.
-
-

TOPIC B

Write a Bash Shell Script

In the last topic, you worked with the basic Bash shell options to perform various tasks. To execute complex tasks using the operating system, it is essential to script a program for the respective task. In this topic, you will write a basic Bash shell script.

An in-depth knowledge of shell scripts is required to understand the working of the Linux system. As a Linux administrator, it is essential for you to work with shell scripts because they enable you to automate routine tasks, saving time and effort.

Shell Scripts

A shell script is a file that contains a list of commands to be read and executed by the shell. Frequently used commands can be stored in a shell script for repeated use. Every shell script starts with a line that designates the interpreter. This line instructs the operating system to execute the script.

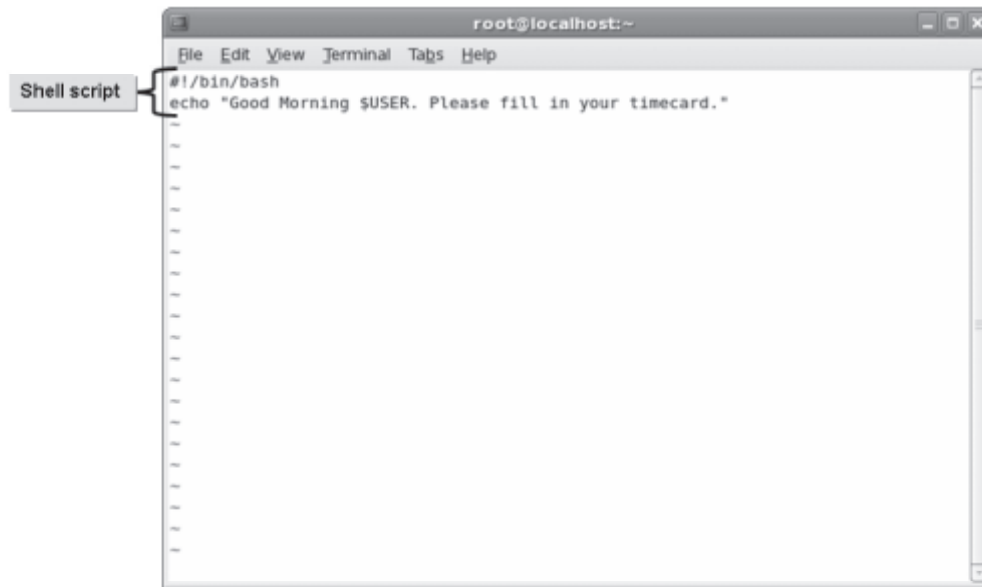


Figure 9-5: Creating a shell script.

Benefits of Scripts

Shell scripts allow you to perform various functions. These functions are listed below.

- Automation of commands and tasks of system administration and troubleshooting.
- Creation of simple applications.
- Manipulation of text or files.

Command Line Operators

The Bash shell facilitates command line expansion, inhibition, and substitution with specific symbols called command line operators. These operators are described in the table.

Operator	Description
\$	Expands variables
'	Substitutes commands
\	Inhibits a single character
!	Substitutes history

#!/bin/bash

Bash scripts contain shell-specific instructions that may not be compatible with other Linux shells. This will result in a Bash script running on certain shells while failing on other Linux shells. To enable Bash scripts to run on all Linux shells, you need to add a line `#!/bin/bash` at the beginning of each script. This line will instruct the operating system to use the Bash shell when executing a script on an incompatible Linux shell.

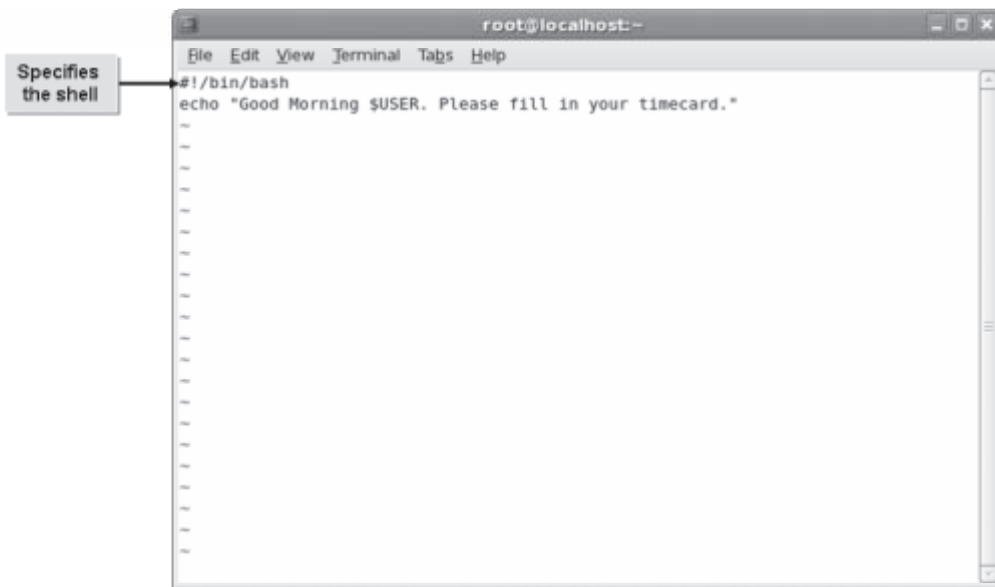


Figure 9-6: `#!/bin/bash` will enable Bash scripts to run on all Linux shells.

The test Command

The `test` command is used to check file types and compare values. You can use the `test` command in your shell scripts to validate the status of files and perform relevant tasks. It evaluates a conditional expression and displays an exit status. The exit status is 0 if the expression is true, 1 if the expression is false, and 2 if an error occurs.



Figure 9-7: The `test` command is used to determine whether a directory is empty or not.

How to Write a Shell Script

Procedure Reference: Write a Bash Script

To write a Bash script:

1. Log in as a user in the CLI.
2. To write a Bash shell script, enter `vi {script file name}`.
3. To switch to insert mode, press **I**.
4. Type `#!/bin/bash` to specify the shell.
5. Type the required command.
6. To return to command mode, press **Esc**.
7. To save the file and exit the text editor, enter `:wq`.

Calling the Correct Interpreter

When you write an sh script, ensure that the first line is `#!/bin/sh`. For a bash script, the first line is `#!/bin/bash`. The first line that contains `#!` is referred to as the shebang line.

Procedure Reference: Convert a Script File to an Executable Script

To convert a file to an executable script:

1. Log in as a user in the CLI.
2. Write a Bash shell script.
3. To convert the file to an executable script, enter `chmod a+x {script file name}`.

Procedure Reference: Execute Scripts Using the Relative Path

To execute scripts using the relative path:

1. Log in as a user in the CLI.
2. Navigate to the directory where the script file is located.
3. To verify that the script file has execute permissions, enter `ls -l`.
4. If necessary, convert the script to an executable script.
5. To execute the script, enter `./{script file name}`.

Procedure Reference: Execute Scripts Using the Absolute Path

To execute scripts using the absolute path:

1. Log in as a user in the CLI.
2. To execute scripts using the absolute path, enter `{absolute path of the script file}/{script file name}`.

Editing a Shell Script

To edit a shell script, open the script file in the vi editor, make the necessary changes to the shell script, and then save the file. The table lists the common default shell scripts and their uses.

If You Need To	Use This Default Shell Script
Set user profile variables	<code>~/.bash_profile</code>
Set user login commands	<code>~/.bash_login</code>
Set global profile variables	<code>~/profile</code>
Set shell variables	<code>~/.bashrc</code>
Set user logout commands	<code>~/.bash_logout</code>
Map the keyboard for situations such as the sound to be played on reaching the end line	<code>~/inputrc</code>

ACTIVITY 9-4


Displaying Directory Content and Time Using Scripts

Before You Begin:

1. You have logged in as root in the CLI.
2. The first terminal is displayed.

Scenario:

You want to remove the unused files on your system. Before proceeding with the cleanup, you want to list the contents of the current working directory. Therefore, you decide to write a script to list directory contents and display the current time simultaneously, to maintain a record of the time of listing.

What You Do	How You Do It
1. Write a simple Bash shell script.	<ol style="list-style-type: none"> To open the script file in the vi editor, enter vi helloworld To switch to insert mode, press I. To specify the shell, enter #!/bin/bash Enter echo "Hello World" Enter echo "The current date and time is : `date`" <p> Ensure that you use back quotes (`) while typing the date command.</p> Type echo "The files in the current directory are \$(ls `pwd`)" To switch to command mode, press Esc. Enter :wq to save the script. Clear the terminal screen.
2. Execute the Bash script.	<ol style="list-style-type: none"> To convert the text file into an executable script, enter chmod a+x helloworld To execute the script, enter ./helloworld less Navigate through the displayed content and observe that the files in the current working directory are listed below with the current date and time. To exit the display, press Q. Clear the terminal screen.

TOPIC C

Customize the Bash Shell

In the last topic, you wrote basic scripts. Now, it's time to configure the Bash shell. Because Linux features multiuser support, you may want to customize the behavior of the Bash shell to suit the requirements of each user and display the user's personal details. In this topic, you will work with shell variables and environment variables to customize the shell environment.

In a network environment, there may be multiple users accessing the same system. You may want to personalize users' systems by customizing the shell environment to display individual user names. It may be tedious to write several scripts to perform this task for every user accessing the system. By using variables in a script file, you can customize the shell environment to display the name of the user logging in. Linux shell variables allow you to automate repetitive functions. Creating automated tasks that take the place of repetitive functions will save valuable time.

Variables

Variables refer to entities whose values change from time to time. Most shell variables are set either by the operating system when you log in, or by the shell when it is initially invoked. When you define a variable in a shell script, it is called a local variable of that particular script. The variable cannot be used directly in the command line or by other scripts. When you export the local variable using the `export` command, it becomes an environment variable, which can be used on the command line or by other scripts.

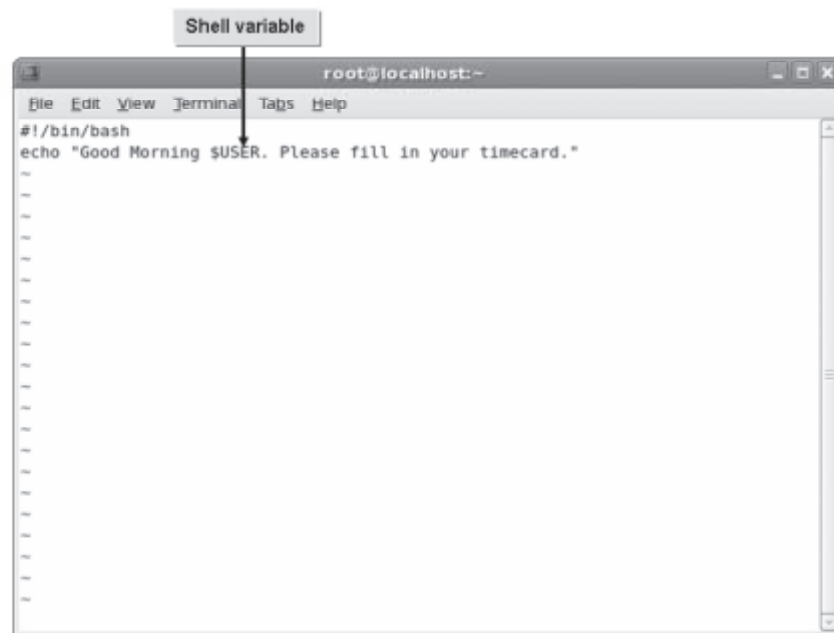


Figure 9-8: Using shell variables in scripts.

Syntax

The syntax of the `export` command is `export {variable}`.

Viewing Variable Values

Variables that are set by the operating system when you log in to a system are automatically exported. Variables created by the shell remain local in scope unless you manually export them. To display the value of a variable, use the `echo` command followed by a dollar sign (`$`) and the variable name (with no space between the `$` and the variable name). For example, to view your default shell, enter `echo $SHELL`. The value of the variable is displayed on the screen. Like Linux commands, the shell variables are also case sensitive.

Declaring Variables

In addition to using and modifying predefined variables, you can also create variables. To create variable names, apply the following rules:

- A variable name must begin with an upper or lowercase letter or an underscore.
- The initial letter or underscore can be followed by any number of additional upper or lowercase letters, numbers ranging from 0 to 9, or an underscore.
- The following character combinations have special meanings and should not be used as variable names or to end a variable name: `$@`, `$#`, `$$`, `$*`, `$-`, `$_`, `$?`, and `$0` to `$9`.

To assign a value to a variable, type the variable name followed by an equal sign and the value (with no spaces). To export a variable, making it accessible to commands and other shells, type `export` followed by the variable you want to export.

Special Shell Parameters

Shells treat some characters specially. Such characters cannot be assigned to variables because they convey special meaning. The following table contains the list of special characters and their description.

Character	Description
<code>*</code>	Signifies the positional parameters, starting from one.
<code>@</code>	Signifies the positional parameters, starting from one. When the expansion occurs within quotation marks, each parameter expands to a separate word. For example, “ <code>\$@</code> ” is equivalent to specifying “ <code>\$1</code> ” “ <code>\$2</code> ”. When there are no positional parameters, “ <code>\$@</code> ” and <code>\$@</code> are removed and do not expand to anything.
<code>#</code>	Signifies the number of positional parameters in decimal.
<code>?</code>	Signifies the exit status of the most recently executed foreground pipeline.
<code>-</code>	Signifies the current option flags as specified upon invocation, by the set built-in command, or those set by the shell itself using the <code>-i</code> option.
<code>\$</code>	Signifies the PID of the shell. In a subshell, it expands to the PID of the invoking shell, not the subshell.

Character	Description
!	Signifies the PID of the most recently executed background command.
0	Signifies the name of the shell or shell script. This is set at shell initialization. If Bash is invoked in a shell script file, \$0 is set as the name of that file.
-	Signifies the absolute path name that is used to invoke the shell or shell script being executed as passed in the environment or argument list.

Working with the CDPATH Variable

In your directory structure, there may be directories that you will want to frequently switch between. By defining the required directory path in the CDPATH variable, you can easily switch to that path.

Environment Variables

An *environment variable* is a storage location in the operating system’s command shell. It is accessible by all programs. An environment variable consists of a name, usually written in uppercase letters, and a value, such as a path name. Environment variables can be directly viewed from the shell.

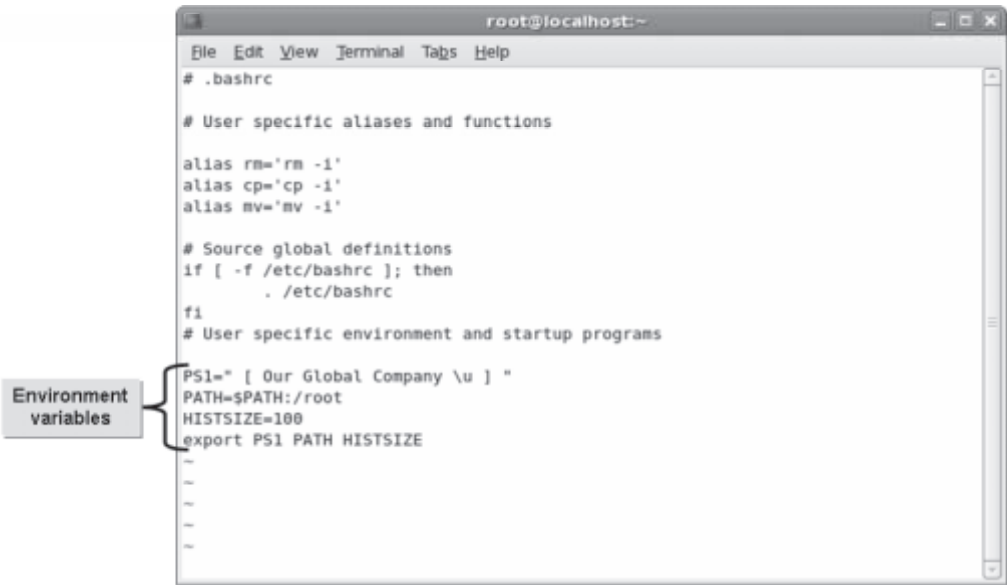


Figure 9-9: Assigning values to environment variables.

Referencing Environment Variables

You can use the existing environment variable in a new or existing shell by referring to it as `${environment variable}`.

Default Environment Variables

Some of the default environment variables and their functions are provided in the following table.

Environment Variable	Description
HOSTNAME={hostname}	Used to specify the hostname of the system.
SHELL={shell path}	Used to specify the shell path for the system.
MAIL={mail path}	Used to specify the path where the mail will be stored.
HOME={home directory}	Used to specify the home directory of the user.
PATH={user path}	Used to specify the path in which the user needs to operate.
HISTSIZE={number}	Used to specify the number of entries to be stored in the command history.
USER={user name}	Used to specify the name of the user.
EDITOR={text editor name}	Used to specify the preferred text editor for the environment.
TERM={terminal name}	Used to specify the name of the terminal used.
PRINTER={printer name}	Used to specify the default printer of the system.
PAGER={command}	Used to specify the command through which the content of long files need to be listed.
PS1=[prompt]	Used to specify the primary prompt—the prompt that is displayed on login.
PS2=[prompt]	Used to specify the secondary prompt.

The alias Command

The *alias* command is used to generate command line aliases. Aliases are shorthand for longer expressions. Using aliases, you can substitute a word in a command with a string. The shell maintains a list of aliases that are created and listed using the `alias` command. It also maintains a list of aliases that are removed using the `unalias` command.

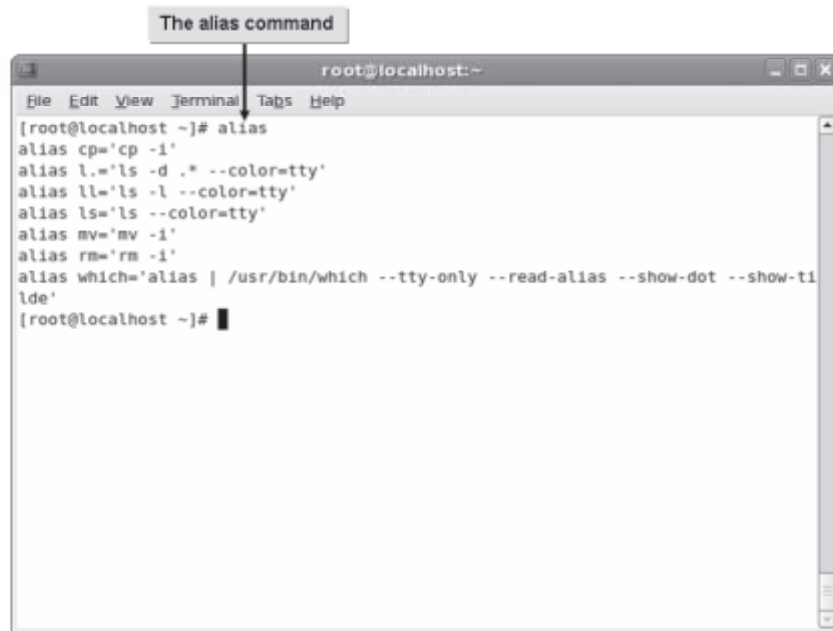


Figure 9-10: Viewing command line aliases.

Syntax

The syntax of the alias command is `alias {alias name}='{command}'`
`[options]'`.

HISTFILESIZE

The HISTFILESIZE environment variable allows you to set the maximum number of lines contained in the history file. It also allows you to specify the number of lines to be displayed on running the history command. For example, on assigning a value of 20 to this variable, the history file gets truncated to contain just 20 lines. The default value to this variable is 1,000.

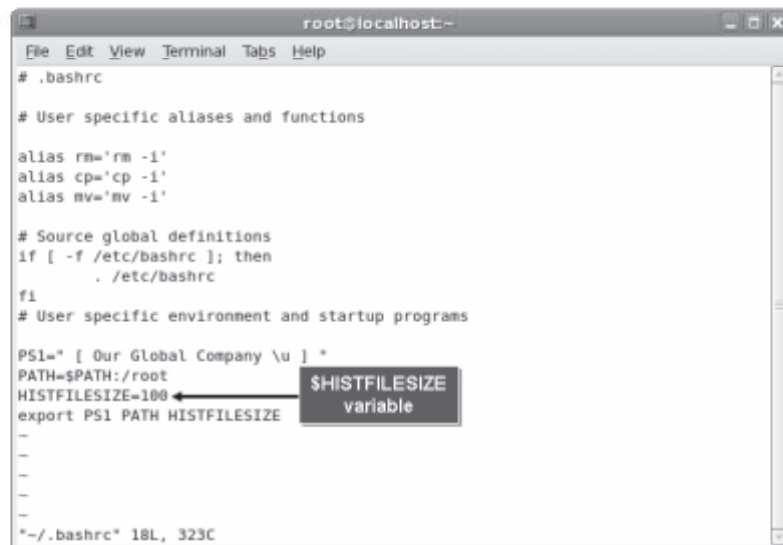


Figure 9-11: Assigning a value to the HISTFILESIZE variable.

SUID Scripts

Definition:

An *SUID script* is a program that overrides normal permissions and runs with the permissions of the owner of the program. The `chmod` command is used to set the SUID to the shell script. Care should be taken to secure the script with the SUID because it is prone to being hacked.

Example:

```

$$ cat ./suid.c
#include <unistd.h>
int main(int argc, char *argv[]) {
    execl("/usr/bin/is", "id", (void*)0);
    return(0);
}
$ cc suid.c -o suid -Wall -O2
$ sudo chown root.wheel ./suid
$ sudo chmod +s ./suid
$ ./suid
uid=1000(sarnold) euid=0(root) gid=1000(sarnold) egid=0(wheel)
groups=1000(sarnold). 0(wheel)

```

The `chmod` command is used to set the SUID to the shell script

Figure 9-12: A sample SUID script.

Shell Spawning

Shell spawning is a process that allows a shell to create a clone of itself. The copy is called the child process. It becomes the new process and can also create more processes, which result in multiple generations of processes. The shell spawns a child process when the user enters a command. The shell waits for the child process to be completed before displaying the prompt again to accept another command.

Search Paths

Definition:

A *search path* is a sequence of various directory paths that is used by the shell to locate files. Paths can be assigned to the *PATH* environment variable. The *PATH* variable comprises a list of directory names separated by colons. You can add a new path to an existing group of path names, modify a path, or delete a path. Usually directories that contain executable files are assigned to the *PATH* variable.

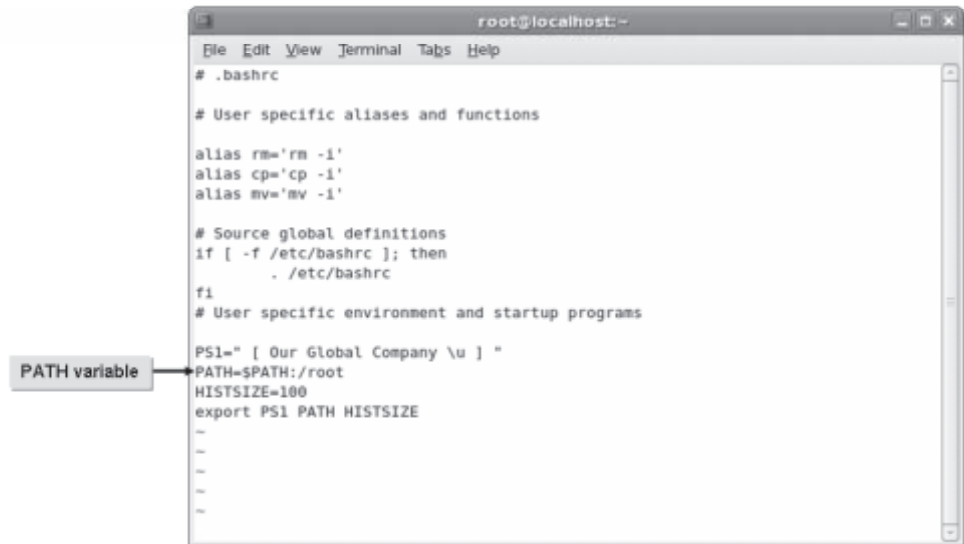


Figure 9-13: A search path defined in the *.bashrc* file.

Example:

The following is an example of a search path where the path names are separated by colons:

```
/home/user/bin:/usr/local/bin:/usr/bin:/bin
```

Non-Example:

The following is not a search path because the path names are not separated by colons:

```
/usr/bin /usr/local/bin
```

How to Use Shell Variables

Procedure Reference: Define Variables

To define variables:

1. Log in as a user in the CLI.
2. To define a variable, enter `{VARIABLE}={value}`.
3. To display the value associated with the variable, enter `echo ${VARIABLE}`.

Procedure Reference: Set an Alias for a Frequently Used Command

To set an alias for a frequently used command:

1. Log in as a user in the CLI.
2. To view the default aliases, enter `alias`.
3. To set an alias for a frequently used command, enter `alias {alias name}='{command}'`.
4. To view the updated alias on the system, enter `alias`.

Procedure Reference: Set Configuration Variables

To set configuration variables:

1. Log in as root in the CLI.
2. To open the `.bashrc` script file, enter `vim ~/.bashrc`.
3. Make the necessary changes such as changing **PS1**, **HISTSIZE**, **PATH**, or **alias**.
4. Export the variables and save the file.
5. For the changes to apply, log out and log in as root.

Procedure Reference: Specify the Script Location to the PATH Variable

To specify a script location to the `PATH` variable:



You can manually add the location of a shell script file to the default `PATH` variable and execute the script from any location.

1. Log in as user in the CLI.
2. Enter `vi {script file name}`.
3. Write the script commands and save the file.
4. To make the file an executable script, enter `chmod a+x {script file name}`.
5. Log out as user and log in as root.
6. Enter `vi .bash_profile`.
7. To add the location of the script file to the default `PATH` variable, in the line starting with “`PATH=`”, move to the end of the line and type `:{location of the script file}`.
8. Save and exit.
9. Log out and log in the CLI.
10. To execute the file, enter `{script file name}`.

Procedure Reference: Add Script to the Location in the PATH Variable

To add script to the default location in the `PATH` variable:



You can manually add the shell script file to the default location specified in the `PATH` variable to execute the script from any location.

1. Log in as user in the CLI.
2. Enter `vi {script file name}`.
3. Write your script and save the file.
4. To convert the file into an executable script, enter `chmod a+x {script file name}`.
5. Log out as user and log in as root.

6. To move the script to the default location in the PATH variable, enter
`mv /home/User/{location of the script file}/{script file name} /{default location of the PATH variable}.`
7. Log out as root and log in as user in the CLI.
8. Enter `{script file name}` to execute the script.

Default Location of the PATH Variable

Whenever you execute a command or script, the system by default searches the location specified in the default PATH variable. Only the commands or scripts present in these locations can be executed from any location.

The default location of the PATH variable for a user is as follows:

- `/usr/local/bin`
- `/bin`
- `/usr/bin`

The default location of the PATH variable for a root user is as follows:

- `/usr/local/bin`
- `/bin`
- `/usr/bin`
- `/usr/local/sbin`
- `/sbin`
- `/usr/sbin`

Procedure Reference: Manage Shell Script Ownership

To manage shell script ownership:

1. Log in as root in the CLI.
2. View the owner of the shell script file.
 - a. Navigate to the directory where the shell script is located.
 - b. To view the ownership of the shell script file, enter `ls -l`.
3. Change the owner.
 - To change the user, enter `chown {user name} {script file name}` or;
 - To change the group owner, enter `chgrp {group name} {script file name}`.

Procedure Reference: Manage Execution of Shell Script

To manage execution of shell script:

1. Log in as a user in the CLI.
2. Navigate to the directory where the shell script is located.
3. To convert the file into an executable script, enter `chmod a+x {script file name}`.
4. Execute the script.
 - Enter `{script file name}`.

- Enter `./{script file name}`.
- Enter `/{directory where the script file is located}/{script file name}`.
- Add the directory path of the script file to the PATH variable in the `~/.bash_profile` file and then log out to apply the setting. Login and enter `{script file name}` or;
- Add the script file to the default location in the PATH variable and enter `{script file name}`.

Procedure Reference: Manage the SUID Rights of Shell Scripts

To manage the SUID rights of shell scripts:

1. Log in as a user in the CLI.
2. Navigate to the directory where the shell script is located.
3. To set the UID to the script file, enter `chmod u+s {script file name}`.

Procedure Reference: Set Environment Variables when Spawning a New Shell

To set environment variables when spawning a new shell:



You can create a new variable and make it available to a new shell or to an existing shell.

1. Log in as root in the CLI.
2. If desired, to view the environment variables, enter `env`.
3. Enter `vi .bash_profile`.
4. Define and export an environment variable at login.
 - a. Switch to input mode.
 - b. To define a variable, enter `{ENVIRONMENT VARIABLE}={value}`.
 - c. To export the variable, type `export {ENVIRONMENT VARIABLE}`.
 - d. Save and close the file.
5. Log out and log in to apply the changes.
6. If necessary, to verify whether the value that was set for the environment variable is applied, enter `echo ${ENVIRONMENT VARIABLE}`.
7. Enter `vi {script file name}`.
8. Enter the script to use the environment variable in a new shell.
 - a. Switch to input mode.
 - b. Enter `#!/bin/bash`.
 - c. To refer the variable and get its value, enter the desired script and use `${ENVIRONMENT VARIABLE}`.
 - d. Save and close the file.
9. To convert the file to an executable script, enter `chmod a+x {script file name}`.
10. To execute the script file, enter `./{script file name}`.

Local and Environment Variables

When you define a variable in a shell script, it is called a local variable of that particular shell script. This cannot be used by other shell scripts or outside that shell script. When you export the local variable using the `export` command, it becomes an environment variable, which can be used by other shell scripts or by the command line.

Referencing Environment Variables

You can use the existing environment variables in a new or existing shell wherever necessary by referring to it as `${ENVIRONMENT VARIABLE}`.

ACTIVITY 9-5

Using Shell Variables in Scripts

Before You Begin:

- 1. You have logged in as root in the CLI.
- 2. The first terminal is displayed.
- 3. Log out of root.

Scenario:

You have been assigned the task of creating a script to remind employees to fill in their timecards at the end of each day. You decide to use variables to define the names of the employees.

What You Do	How You Do It
1. Create the Filltimecard file.	<div>a. Log in as <code>jsmith</code>.</div> <div>b. To create a file named Filltimecard, enter <code>vim Filltimecard</code></div> <div>c. Switch to insert mode.</div> <div>d. To specify the shell, enter <code>#!/bin/bash</code></div> <div>e. To specify the variable, enter <code>USER='whoami'</code></div> <div>f. To set the reminder, type <code>echo "Good Evening \$USER. Please fill in your timecard."</code></div>

2. Save and convert the file into an executable script.
 - a. Switch to command mode.
 - b. Save and close the file.
 - c. To convert the file into an executable script, enter `chmod a+x Filltimecard`
 3. Test the script.
 - a. To view the contents of the file, enter `cat Filltimecard`
 - b. To execute the script, enter `./Filltimecard`
 - c. Compare the results with that of the `cat` command. Observe that your user name appears in place of the `USER` variable.
 - d. Clear the terminal screen.
 - e. Log out of the `jsmith` user account.
-

ACTIVITY 9-6

Customizing Systems Using Variables

Before You Begin:

The login screen of the first CLI terminal is displayed.

Scenario:

As an administrator, you need to set up Linux systems for new employees. Before the completion of the setup process, you have to customize the systems with the following details:

- The command prompt should reflect the company name.
- The `Filltimecard` script should be assigned a local path on the system.
- The command history should display the last 100 entries.

LESSON 9

What You Do	How You Do It
1. Set the command prompt to reflect your company name.	<ol style="list-style-type: none">Log in as root.To open the <code>~/.bashrc</code> file, enter vim ~/.bashrcTo change the primary prompt, on a new line, enter PS1=" [Our Global Company \u] "
2. Set the file path and the history file size.	<ol style="list-style-type: none">To assign the path, where the Filltimecard script is located, to the PATH variable, enter PATH=\$PATH:/rootTo assign a value of 100 to the history file content, enter HISTSIZE=100
3. Export the variables and save the changes made to the file.	<ol style="list-style-type: none">To export the three variables, type export PS1 PATH HISTSIZESwitch to command mode.Save and close the file.
4. Check the changes.	<ol style="list-style-type: none">Log out of the root user account.To verify the change, log in as rootObserve that the prompt now displays the company name. To view the command history, enter history lessNavigate through the history display. Observe that only the last 100 entries (excluding the latest command) are displayed.Quit the history page. Clear the terminal screen.

TOPIC D

Redirect Standard Input and Output

In the previous topic, you performed shell scripting using variables. As part of automating tasks using scripts, you may now want to manipulate the input and output of Linux commands and files. In this topic, you will redirect standard input and output.

Imagine that you need to create a troubleshooting report, which contains a command and the respective errors it generates after execution. In this situation, instead of keying the output or errors in the report, you can redirect the output of the command into the report. Redirection techniques help you accomplish certain tasks with speed and ease.

Standard Input

Standard input, or *STDIN*, is a *text stream* that acts as the source for command input. Usually standard input for the Linux command line is from the keyboard. In the case of the GUI, the standard input can also be from the mouse. The standard input stream is buffered and lends itself to be redirected.



Figure 9-14: Standard input entered using the keyboard.

The read Command

The `read` command is used to read content from the standard input, the keyboard, and assign it to a variable.

Standard Output

Standard output, or *STDOUT*, is a text stream that acts as the destination for command output. By default, standard output from the Linux command is directed to the terminal screen. The standard output stream is buffered and lends itself to be redirected.



Figure 9-15: Standard output displayed on the terminal.

The seq Command

The *seq* command prints a sequence of numbers on the standard output. It allows you to specify a start value, an end value, and an incremental value. The syntax of the *seq* command is: *seq [start value] [increment value] {end value}*. For example, *seq 12* will display numbers from 1 to 12, while *seq 2 500* will display all the odd numbers from 1 to 500.

Standard Error

Standard error, or *STDERR*, is a text stream that is used as the destination for error messages. The *STDERR* stream is not buffered. By default, the standard error stream prints error messages on the terminal screen, but this can be changed by redirecting it to the desired location.

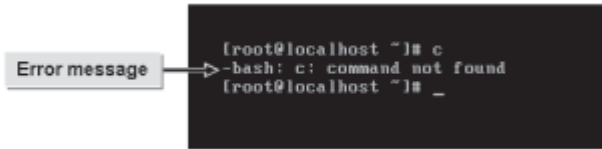


Figure 9-16: Standard error message displayed on the monitor.

Redirectors

A *redirector* is an operator that accepts input data from a source other than the keyboard or sends data to a destination other than the monitor. It generally uses files as input or output. A redirector can redirect the output of a command to serve as the input for another command. It can also send output data to both the screen and a file.

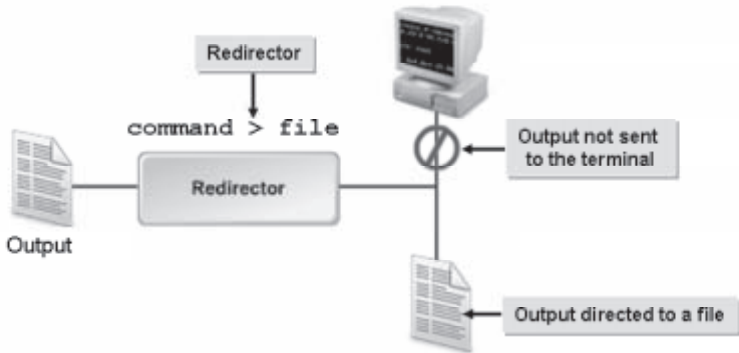


Figure 9-17: Output from a command redirected to a file.

There are some operators that are used to redirect input or output. The functions of frequently used operators are described in the following table.

Operator	Enables You To
>	Redirect the standard output to another file.
>>	Append the standard output to the end of the destination file.
2>	Redirect the standard error message to a file.

Operator	Enables You To
2>>	Append the standard error message to the end of the destination file.
&>	Direct all the output of a command to a file.
<	Read the input from a file rather than from the keyboard or mouse.
<<string	Provide input data from the keyboard, indicating the end with the specified string.
=	Assign values to variables.
= =	Check if two values are equal to each other.

 The semicolon (;) is used to separate variables, commands, or values.

Examples of Redirection

`mail < myletter.txt`—The myletter.txt file will be taken as the input.

`ls > file1.txt`—The output of the `ls` command will be redirected to a file named file1.txt.

`ls file3.txt 2> errorfile.txt`—Assuming that file3.txt does not exist, the resulting errors will not be displayed on the screen, but they will be redirected to a file named errorfile.txt.

The Pipe Operator

Definition:

The *pipe* is an operator that combines commands. It uses the standard output of one command as the standard input for another command. The output format of the first command should be compatible with the format that the second command works with. The pipe operator can be used with most commands in Linux.

Example:

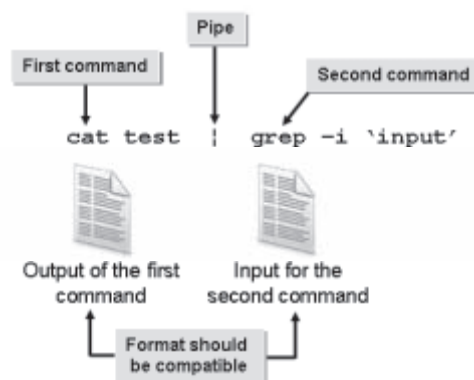


Figure 9-18: The pipe operator is used to combine two Linux commands.

Example of Commands Using the Pipe Operator

`ls | more`—The output of the `ls` command is the input for the `more` command.

Lists in Shell Scripts

In shell scripts, you can write scripts to execute a number of commands in sequence by creating a list. This list can be created by using one of the four symbols, “;”, “&”, “&&”, or “||” to separate the commands. You can use “;” or “&” as the terminal character.

The operators used in shell scripts are listed below.

Operator	Description
;	Separates commands and they will be executed one after the other.
&	Executes the preceding pipeline as a background task.
&&	Executes only if the preceding command or pipe is terminated normally.
	Executes only if the preceding command or pipe terminated with an error.

The xargs Command

The `xargs` command constructs and executes command lines. The pipe operator is used to make the output of the first command the input for the second command. The `xargs` command adds arguments from the standard input to complete the command and then executes it.

The `xargs` command has various options.

Option	Used To
<code>-I {replacement string_}</code>	Consider each line in the standard input as a single argument.
<code>-L {number of lines}</code>	Read a specified number of lines from the standard input and concatenate them into one long string.
<code>-p</code>	Prompt the user before each command.
<code>-n {number}</code>	Read the maximum number of arguments from the standard input and insert them at the end of the command template.
<code>-E {end of string}</code>	Represent the end of the standard input.
<code>-t</code>	Write each command to the standard error output before executing the command.
<code>-s {maximum allowable size}</code>	Set the maximum allowable size of an argument list to a specified number of characters.

Option	Used To
-x	Terminate the xargs command if it creates a command that is longer than the arguments given in the -n option, is longer than the number of lines given in the -L option, or is longer than the size given by the -s option.

The tee Command

The `tee` command reads the standard input, sends the output to the standard output device, and also copies the output to each specified file. This command enables users to log the output of a command in a file before sending it as the input to the next command; therefore, it serves as a helpful tool in troubleshooting. When used with the `-a` option, it appends the output to each output file instead of overwriting it. When used with the `-i` option, it ignores interrupt signals.

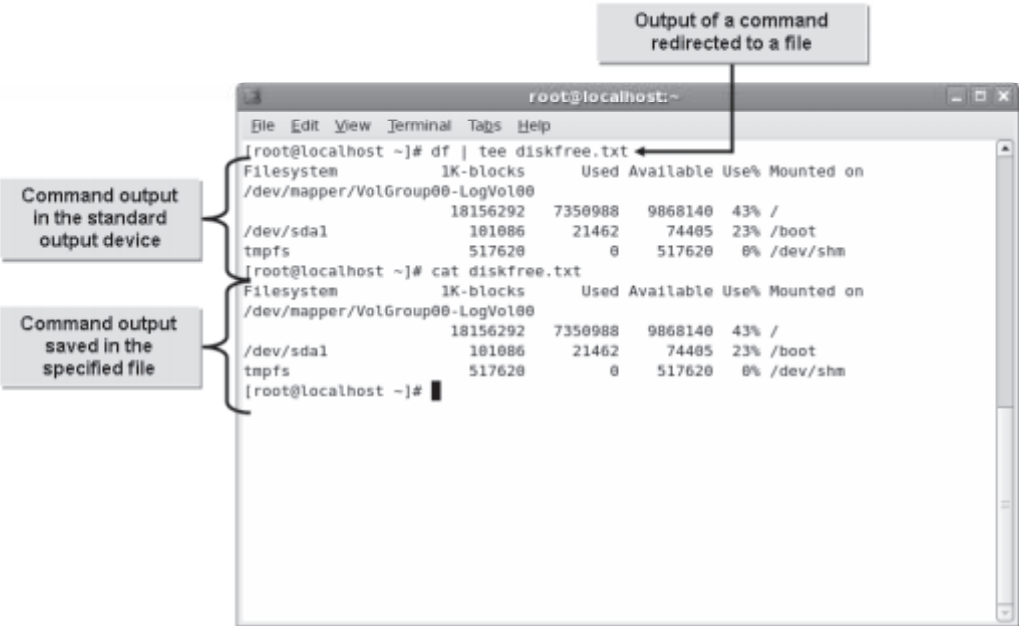


Figure 9-19: Output of the `df` command redirected to a file.

Command Substitution

Command substitution is the ability to reassign the output of a command as an argument to another command. The command line that needs to be reassigned is placed within back quotes (`' '`). First, the shell executes the commands enclosed within the back quotes. Then, it replaces the entire expression, including the back quotes, with the output of the command.

Single Quotation Marks and Quotation Marks

Single quotation marks (`' '`) are used in a shell command to disable any kind of transformation or modification. The shell considers whatever is enclosed within the single quotation marks as a single entity or parameter. If single quotation marks are used, substitution will not take place.

By employing quotation marks (" "), the expansion of the file name is suppressed by the shell. Even if a wildcard, such as the asterisk (*), is enclosed within quotation marks, the standard feature of the wildcard (matching all characters) will be lost.

How to Redirect Input and Output

Procedure Reference: Redirect the Standard Output to a File

To redirect the standard output to a file:

1. Log in as a user.
2. Redirect the standard output to a file.
 - To direct the standard output of the command to the specified file, at the command prompt, enter `{command} > {file name}`.
 - To append the standard output of the command to the end of the specified file, enter `{command} >> {file name}`.

Procedure Reference: Redirect the Standard Error as Output to a File

To redirect the standard error as output to a file:

1. Log in as a user.
2. Redirect the standard error to a file.
 - To direct the error message from the command to the specified file, enter `{command} 2> {file name}`.
 - To append the error message from the command to the end of the specified file, enter `{command} 2>> {file name}`.

Procedure Reference: Redirect the Standard Output to a Command

To redirect the standard output to a command:

1. Log in as a user.
2. To redirect the output of one command as input to another command, enter `{command 1} | {command 2} | {command 3}`.

Procedure Reference: Redirect the Standard Output to a File and Command

To redirect the standard output to a file and command:

1. Log in as a user.
2. To save the output at various stages in files and direct the output to other commands, enter `{command 1} | tee {file name 1} | {command 2} | tee {file name 2} | {command 3}`.

Procedure Reference: Redirect the Standard Output and the Standard Error to a File and Command

To redirect the standard output and the standard error to a file and command:

1. Log in as a user.
2. Redirect the standard output and the standard error.

- To direct the standard output of the command to a file and the standard error message to another file, enter `{command} > {file name 1} 2> {file name 2}`.
- To direct all the output of the command to a file, enter `{command} &> {file name}`.
- To direct all the output of the command and the standard error messages to another command, enter `{command 1} 2>&1 | {command 2}`.

Procedure Reference: Redirect the Standard Input

To redirect the standard input:

1. Log in as a user.
2. Redirect the standard input.
 - To send a file as the input to a command, enter `{command} < {file name}`.
 - To accept input from the keyboard until a specified string is provided as input, enter `{command} <<{string}`.

ACTIVITY 9-7

Redirecting Content

Data Files:

- Hardwareinventory.txt
- Softwareinventory.txt

Before You Begin:

1. You have logged in as root in the first terminal of the CLI.
2. To open the `~/.bashrc` file, enter `vim ~/.bashrc`.
3. Remove the line starting with “PS1=.”
4. Remove PS1 from the line starting with “export.”
5. Save and close the file.
6. Log out and log in as root
7. Clear the terminal screen.

Scenario:

On the main server of your company, the data related to software inventory and hardware inventory are stored as separate files. You have been assigned the task of consolidating these files into a new file named `Inventory.txt` so that it can be viewed online.

LESSON 9

What You Do

How You Do It

1. Redirect the contents of the Softwareinventory.txt and Hardwareinventory.txt files to the Inventory.txt file.

- a. To create an empty file named Inventory.txt, enter **touch Inventory.txt**
- b. To redirect the contents of the Softwareinventory.txt file to the Inventory.txt file, enter **cat Softwareinventory.txt > Inventory.txt**
- c. To view the contents of the Inventory.txt file, enter **cat Inventory.txt**
- d. Clear the terminal screen.
- e. To append the contents of the Hardwareinventory.txt file to the Inventory.txt file, enter **cat Hardwareinventory.txt >> Inventory.txt**

2. View the Inventory.txt file.

- a. To view the pagewise contents of the Inventory.txt file, enter **cat Inventory.txt | less**
- b. Press the **Spacebar** two times to navigate through the remaining pages in the file.
- c. To exit and return to the shell prompt, press **Q**.
- d. Clear the terminal screen.

TOPIC E

Use Control Statements in Shell Scripts

In the last topic, you redirected the standard input and output between commands and files. Now, you may want to write a simple shell script to automate repetitive tasks. In this topic, you will use control statements in shell scripts.

Consider a scenario where you want to greet users by displaying either “Good Morning,” “Good Afternoon,” or “Good Evening,” according to their login time. Using control statements, you can specify the time span for each message and display the relevant message depending on the time the user logs in.

Control Statements

A *control statement* is an instruction that determines the direction a program takes depending on a test condition. The direction can be different from the sequential order in which the instructions are listed. Control statements are associated with one or more action statements that will be executed only when a specified condition is satisfied.

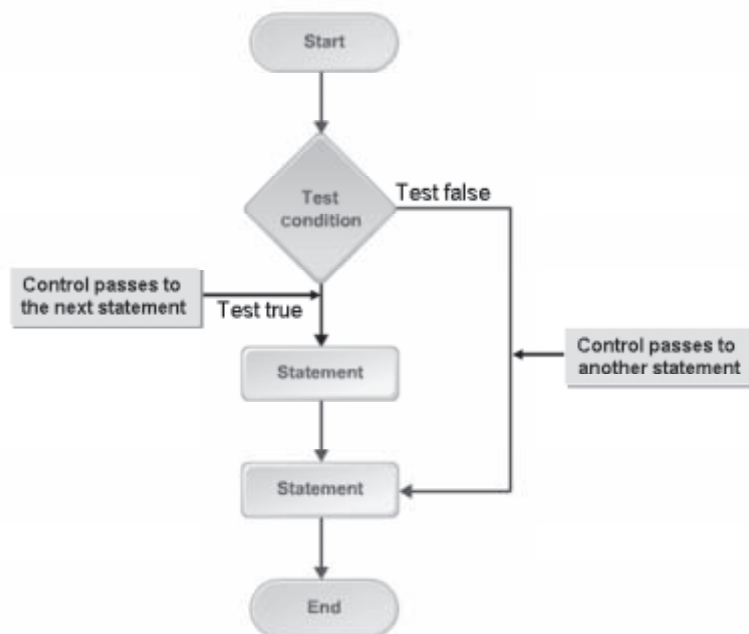


Figure 9-20: Control statements are used to change control flow.

Expressions

Expressions are a group of characters that are generally used to specify conditions. They are formed by combining variables and constants with operators. They are used in the `if` and `while` statements. Performing arithmetic comparisons and string comparisons and testing files are the main functions of expressions. If an expression contains the `<`, `>`, `&`, or `|` symbol, parentheses are required.

Programming Constructs

Definition:

Programming constructs are parts of a program that define the order in which the instructions in a program are executed. A programming construct is a sequence of statements that starts with a command, such as `if`, and ends with the corresponding terminal statement. Constructs may or may not return a value.

Example:

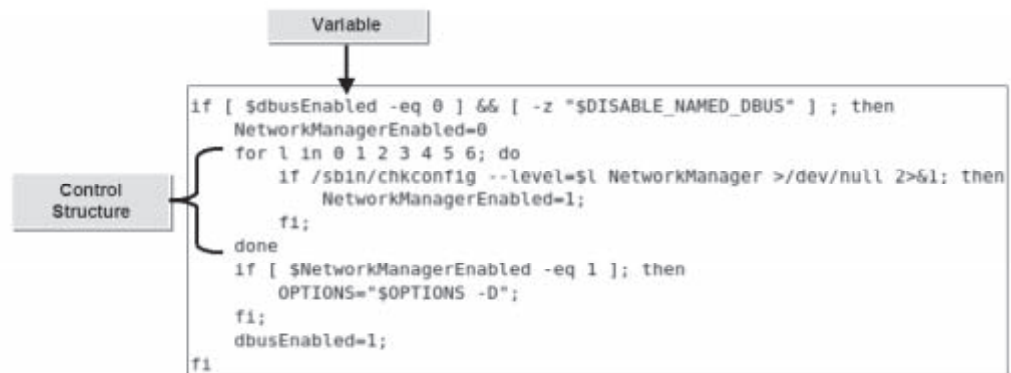


Figure 9-21: A sample programming construct used in system scripts.

Loops

A *loop* is a programming construct that supports repetitive execution of one or more statements. It is a block of code that repeats a list of commands as long as the condition controlling the loop is true.

Test Constructs

In a programming language, *test constructs* test for a condition and then act according to the result of the test. An `if` programming construct tests a list of commands to check whether their exit status is 0. If yes, one or more commands are executed. Bash also uses the `test` command and various bracket and parentheses operators as test constructs.

Functions

Definition:

A *function* is a subprogram that executes an operation and returns a value on completion of the operation. Functions take variables, called arguments, as input. There are two types of functions: built-in functions and user-named functions. Functions can also execute other functions.

Example:

```
# /etc/profile

# System wide environment and startup programs, for login setup
# Functions and aliases go in /etc/bashrc

pathmunge () {
    if ! echo $PATH | /bin/egrep -q "(^|:)$1($|:)" ; then
        if [ "$2" = "after" ] ; then
            PATH=$PATH:$1
        else
            PATH=$1:$PATH
        fi
    fi
}
```

Figure 9-22: *A sample function.***Variables**

A variable is a named storage location in a program's memory that can be assigned a value. Variables can hold different values at different times, but only one value at a time. User-defined variables, as suggested by the name, are defined by the user and are local to the current shell. System variables are those that are created and maintained by the operating system itself.

Comparison and Logical Operators

Some comparison, logical, and arithmetic operators are listed in the tables.

If You Need To	Use This Operator
Check if both values are equal.	==
Check whether the first value is greater than the second value.	>
Check whether the first value is less than the second value.	<
Check if both values are unequal.	!=
Check whether the first value is greater than or equal to the second value.	>=
Check whether the first value is less than or equal to the second value.	<=

Logical Operator	Description
&&	Boolean AND
	Boolean OR
^	Boolean XOR
!	Boolean NOT

If You Need To	Use This Arithmetic Operator
Increase the value by one.	++
Decrease the value by one.	--

The if Statement

The most frequently used construct is the `if` statement. An `if` statement contains a condition to be evaluated and one or more actions to be performed, if the condition is satisfied. If the condition is not satisfied, the actions are skipped and the next statement in the script is executed. The end of the set of instructions is indicated by the `fi` statement.

Syntax

The syntax for the `if` statement is as follows:

```
if ( {condition that needs to be satisfied} )
then
{commands to be executed}
..
fi
```

The if...else Statement

The `if...else` statement allows a choice between two actions based on the evaluation of a condition. If the condition is satisfied, the first action is performed; otherwise, the action following the `else` segment is performed. The end of the set of instructions is indicated by the `fi` statement. If there are more than two sets of instructions, one or more `elif` statements may be used to specify alternative sequences of action.

Syntax

The syntax for the `if...else` statement is as follows:

```
if ( {condition that needs to be satisfied} )
then
{commands to be executed}
..
else
{commands to be executed}
..
fi
```

Looping Statements

Looping statements, also referred to as iterative statements, are a type of control statements that help you execute a part of the script repeatedly based on a specific condition that is evaluated. The condition is tested based on the value of a variable. There are two types of loops supported by the Bash shell: the `for` loop and the `while` loop. In shell scripts, the commands to be iterated are enclosed within the `do` and `done` statements.

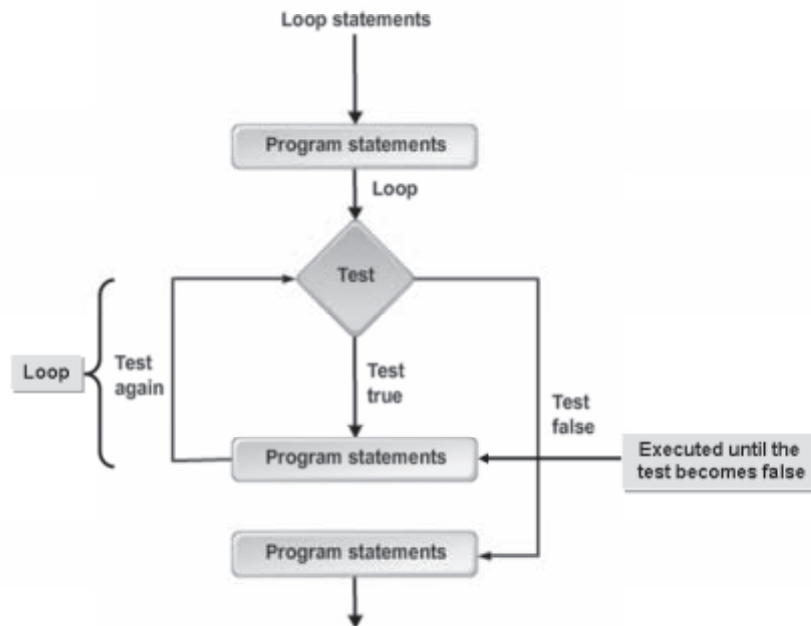


Figure 9-23: Loop statements are used to repeat a set of instructions.

The for Loop

The *for* loop executes a part of the script as many times as specified by a numerical variable that is within the conditional part of the statement. The *for* loop is unique because the conditional part of the statement contains the initial value of the variable, the test condition, and the increment or decrement of the variable value.

Syntax

The *for* loop in Linux lets you repeat a series of commands based on the evaluation of a condition. For example, the syntax for a *for* loop is as follows:

```
for (( {expr1}; {expr2}; {expr3} ))
do
{commands to be executed}
..
done.
```

In this syntax, *expr1* is the initial statement executed once before the first loop, *expr2* is the test condition, and *expr3* is the increment or decrement expression that is executed at the end of each loop.

Alternate syntax: The *for* loop has another syntax:

```
for {variable name} in {list}
do
{commands to be executed}
..
done.
```

In this syntax, the variable is assigned a value from the list and the loop executes once for each value given in the list.

The while Loop

The *while* loop enables you to repeat a set of instructions for a fixed number of times, while a specific condition is met. The condition is left open ended in a *while* loop. The first expression is evaluated, and if the expression is true, the actions in the loop are performed. The execution returns to the beginning of the loop and the expression is evaluated again. If the expression is false, the execution passes to the next statement.

Syntax

The syntax for a *while* loop is as follows:

```
while { condition that needs to be satisfied }
do
{commands to be executed}
..
done.
```

The until Loop

The *until* loop is similar to the *while* loop, except that the code is executed when the control expression is false. For example, the syntax for an *until* loop is as follows:

```
until ( {condition that needs to be satisfied} )
do
{commands to be executed}
..
done.
```

How to Use Control Statements

Procedure Reference: Use Control Statements in Scripting

To use control statements in scripting:

1. Log in as a user.
2. To write a Bash shell script, on a terminal, enter `vi {script file name}`.
3. To switch to insert mode, press **I**.
4. Type `#!/bin/bash` to specify the shell.
5. Enter the commands you want to execute.
6. Use control statements or loops, as necessary.
 - To use the `if` statement, type

```
if ( {condition that needs to be satisfied} )
then
{commands to be executed}
fi.
```


- To use the `if...else` statement, type


```
if ( {condition that needs to be satisfied} )
then
{commands to be executed}
else
{commands to be executed}
fi.
```
 - To use the `for` loop, type `for (({expr1}; {expr2}; {expr3}))`

```
do
{commands to be executed}
..
done.
```
 - To use the `while` loop, type


```
while
[{condition that needs to be satisfied}]
do
{commands to be executed}
done.
```
7. To return to command mode, press **Esc**.
 8. To save the file and exit the text editor, enter **:wq**.
 9. To convert the file to an executable script, enter `chmod a+x {script file name}`.

Procedure Reference: Email the Superuser Based on Command Return Values

To conditionally email the superuser based on command return values:



You can automatically send an email message to the superuser or administrator based on the condition specified in the script file. When the specified condition is satisfied by the system, an email message will be forwarded to the superuser. The root user is also called the superuser.

1. Log in as a user.
2. To email the superuser, type the script.
 - a. Enter `vi {script file name}`.
 - b. Type `if ((conditions)) then` and press **Enter**.
 - c. To define a value to a variable, enter `{variable}={value}`.
 - d. Enter `fi`.
 - e. Enter `if [${variable name} = {value}] then`.
 - f. Enter `echo "Type the body of the mail"`.
 - g. To send an email to the root user with the specified subject, enter `mail -s "{subject of the mail}" root`.
 - h. Enter `fi`.
 - i. Save and close the file.
3. To convert the file to an executable script, enter `chmod a+x {script file name}`.
4. To execute the script, enter `./{script file name}`. If the given condition is satisfied, the message, "Type the body of the mail," is displayed.

5. Type the body of the message and, on the last line, enter a period to terminate the email.
6. If necessary, enter the `Cc:` address.
7. Verify that the specified superuser has received the email message.
 - a. Log in as the superuser.
 - b. To open the mailbox, enter `mail`.
 - c. To read the mail's contents, type the mail number.

Identifying a New Email Message

You can identify a new email message by the `>N` symbol at the beginning.

Procedure Reference: Write a Bash Function for Frequently Used Sequence of Commands

To write a bash function for frequently used sequence of commands:

1. Log in as root in the CLI.
2. Write a bash function for a sequence of commands.
 - a. Enter `vi /{bash function name}`.
 - b. Enter `#!/bin/bash`.
 - c. Enter a sequence of frequently used commands using the desired programming constructs. For example, write a program for the `for` loop to automate a sequence of commands.
 - d. Save and close the file.
3. To convert the file to an executable script, enter `chmod a+x {script file name}`.
4. To execute the sequence of commands, enter `./{bash function name}`.

ACTIVITY 9-8

Writing a Script to Create Multiple Directories

Before You Begin:

You have logged in as root in the first terminal of the CLI.

Scenario:

You want to create individual work directories for all employees. Because the task of creating directories individually is time consuming, you decide to write a shell script to automate the process.

Following are the details for writing the Bash script:

- Name of the script: `createdir`
- Prompt text to remind the users to enter the number of directories required:
Specify the number of directories to be created
- Name of the variable to get the total number of directories: `Numberofdir`
- Name of the variable to be used in the `for` loop to store the number of directories: `d`

What You Do	How You Do It
1. Set the total number of directories.	<ul style="list-style-type: none">a. To open a new file for the script, enter <code>vim createdir</code>b. Switch to insert mode.c. To begin the shell, enter <code>#!/bin/bash</code>d. To specify the message to prompt users, enter <code>echo "Specify the number of directories to be created:"</code>e. To read input from users, enter <code>read Numberofdir</code>

LESSON 9

2. Write the loop for creating directories.
 - a. To specify the loop condition, enter **for ((d = \$Numberofdir ; d > 0 ; d--))**
 - b. To indicate the beginning of iterated steps, enter **do**
 - c. To create a directory, enter **mkdir Directory-\$d**
 - d. To indicate the end of the iterated steps, type **done**
 - e. Switch to command mode.
 - f. Save and close the file.
 - g. Clear the terminal screen.

3. Execute the createdir script.
 - a. To convert the file to an executable script, enter **chmod a+x createdir**
 - b. To execute the script, enter **./createdir**
 - c. To create ten directories, enter **10**
 - d. Clear the terminal screen.

4. Check whether the directories are created.
 - a. To view the directories that have been created, enter **ls**
 - b. Observe that ten new directories are listed on the screen.
 - c. Clear the terminal screen.

Lesson 9 Follow-up

In this lesson, you customized the Bash shell and performed various operations in it. You also worked with shell scripts, redirected input and output in shells, and used control statements in scripts to automate repetitive tasks. This will enable you to efficiently perform your job as a system administrator.

1. Why do you use variables in scripts?
2. What are the most prominent features of the Bash shell? Explain.
3. What are the various tasks you can perform by running a shell script?

LESSON 10

Managing Jobs and Processes

Lesson Time

1 hour(s), 30 minutes

In this lesson, you will manage jobs and processes.

You will:

- Manage jobs and background processes.
- Manage processes using the process table.
- Work with delayed and detached jobs.
- Schedule jobs.
- Maintain the system time.

Introduction

In the last lesson, you worked with shells and shell scripts in the Linux environment to help successfully manage a system. In your routine management of a Linux system, there might also be instances when various utilities need to be run simultaneously on a system, not necessarily via shell scripts. In this lesson, you will manage jobs and processes.

The multitasking capability of Linux enables you to perform many tasks, such as compiling a program; sorting a database; and creating a document, at the same time. When system resources are utilized simultaneously, system performance reduces. A system administrator should be able to manage system resources effectively by allocating the right amount of resources to every task run by users.

This lesson covers all or part of the following CompTIA Linux+ Powered by LPI certification objectives:

- Topic A:
 - Objective 103.5
- Topic B:
 - Objective 101.3, Objective 103.5, Objective 103.6
- Topic C:
 - Objective 103.5
- Topic D:
 - Objective 107.2
- Topic E:
 - Objective 105.1, Objective 107.3, Objective 108.1

TOPIC A

Manage Jobs and Background Processes

In the last lesson, you set up Linux variables and executed shell scripts to assist you in daily management of your Linux system. There are, however, other daily tasks that you need to manage in order to run and oversee a Linux system, particularly one that handles multiple users. For example, you may need to manage many processes that can run simultaneously in a Linux environment. In this topic, you will manage multiple jobs and background processes.

Most systems can handle one user running multiple processes, but what happens when hundreds of users run applications simultaneously? As an administrator in such an environment, you need tools and options that allow you to manage system resources efficiently. Using Linux's multitasking capabilities, you can manage jobs and processes in the background.

Processes

Definition:

A *process* is an instance of a running program that performs a data processing task. A process consists of a sequence of steps stored on a system; these steps convert input data to output data. Processes can be subdivided into threads. Every process is assigned a unique PID and includes time limits, shared memory, or child processes. Processes may run in the foreground or background of the system.

Example:

PID	TTY	STAT	TIME	COMMAND
1	?	Ss	0:00	init [5]
2	?	S<	0:00	[migration/0]
3	?	SN	0:00	[ksoftirqd/0]
4	?	S<	0:00	[watchdog/0]
5	?	S<	0:00	[events/0]
6	?	S<	0:00	[khelper]
7	?	S<	0:00	[kthread]
10	?	S<	0:00	[kblockd/0]
11	?	S<	0:00	[kacpid]
67	?	S<	0:00	[cqueue/0]
70	?	S<	0:00	[khubd]
72	?	S<	0:00	[kseriod]
134	?	S	0:00	[pdflush]
135	?	S	0:00	[pdflush]
136	?	S<	0:00	[kswapd0]
137	?	S<	0:00	[aio/0]
290	?	S<	0:00	[kpsmouse]
320	?	S<	0:00	[npt_poll_0]
321	?	S<	0:00	[scsi_eh_0]
324	?	S<	0:00	[ata/0]
325	?	S<	0:00	[ata_aux]
330	?	S<	0:00	[kstripped]
339	?	S<	0:00	[ksnapd]
350	?	S<	0:00	[kjournald]

Figure 10-1: PIDs of processes running on a system.

The Process ID

Whenever a process is started, the system allocates a unique ID, called the PID, to identify the process. Also, every process inherits the UID and GID of the user who starts the process. This is similar to the ownership of files and directories on the Linux filesystem.

The init Process

The first process, called *init* in Linux, is started by the kernel at boot time and never terminates. The PID of the *init* process is always 1.

Foreground Processes

A *foreground process* is a program with which a user interacts at a particular time. Only one foreground process can be run at a time. As the user switches between programs, different programs become the foreground process at different times. A foreground process is initiated by entering a command at the prompt or by clicking a shortcut in the GUI.

Background Processes

A *background process* is a program that allows the Linux shell to execute a command that runs a job in the background, enabling processes to run simultaneously. While the user is interacting with the foreground process, a number of programs can run as background processes. The shell does not have to wait for one process to end before it can run more. A process can be run in the background by suffixing the invoking command with an ampersand (&) separated by a space.

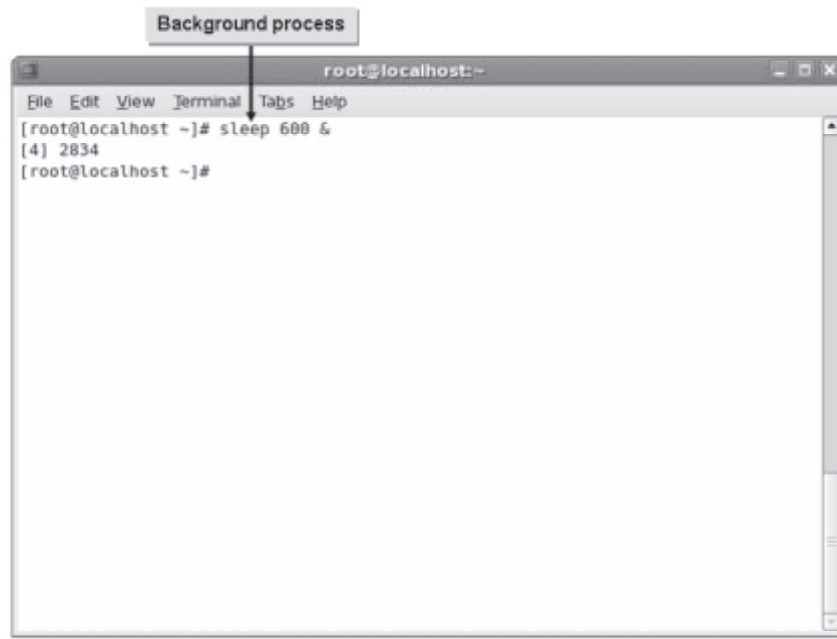


Figure 10-2: A process initiated to run in the background.

Daemons

Daemons always run as background processes that never require user input. Other processes remain in the background temporarily, while the user is busy with the current foreground process.

The Program and Process Relationship

A *program* is a set of instructions describing how to carry out a task. A command that resides on your system is a program. When you enter a command at the prompt, a set of instructions perform a task.

A process is a program that executes instructions. The operating system creates a process to carry out that task. Processes have unique identities and exist until their tasks are completed. When the task is completed, the process is terminated. Each program running on a system is assigned a PID.

Multitasking

Definition:

Multitasking is a method of allowing the operating system to run concurrent programs simultaneously without degrading system performance. Multitasking enables several programs to share the same system resources. Processes spawned by multitasking are all active at the same time. They are not in a sequence or a suspended state waiting to be run. Processes placed in a multitasking state remain active until completed, unless terminated or suspended by the user. One or more users may run multiple tasks on a system.

Example:

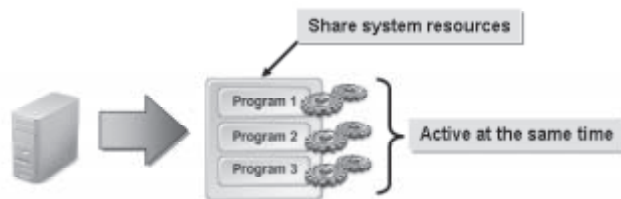


Figure 10-3: Multitasking on a Linux system.

The Jobs Table

The *jobs table*, invoked by the `jobs` command, is a table containing information about jobs running in the background. It contains entries only for those jobs that are running in the current shell. The jobs table contains a numeric label for each job indicating the order in which the jobs were started. In addition, the jobs table includes a plus sign (+) to designate the current or the most recently started job and a minus sign (-) to designate the job that was started just prior to the most recent job. It also includes the status and name of each job.

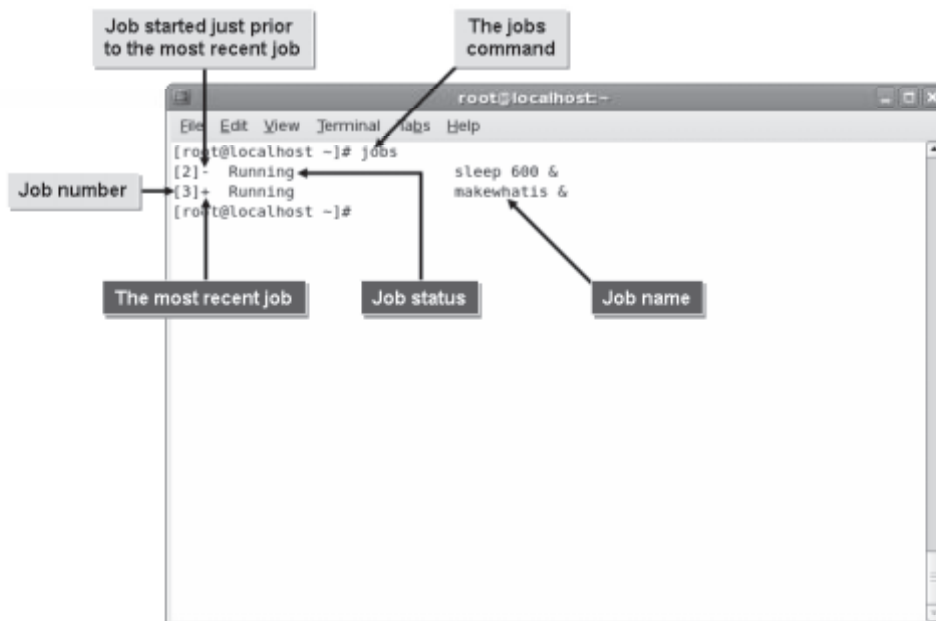


Figure 10-4: The jobs table listing jobs running in the current shell.



The job name listed in the jobs table is actually the command that initiated the job.



The plus (+) and minus (-) signs indicate only the order in which jobs are started. All jobs, however, are actually run simultaneously.

Job Status

There are four possibilities for the status of a job.

Status	Description
Running	An active job.
Stopped	A job that is suspended.
Terminated	A job that is killed.
Done	A completed job.

Jobs in a New Shell

Any job that a user placed in the background will appear in that user's jobs table, but other users' jobs will not appear. If you were to start a new shell, the jobs table for the new shell will be empty. However, the jobs started in the previous shell will continue to run.

Suspend vs. Terminate a Process

The **Ctrl+Z** key combination suspends a job, while the **Ctrl+C** key combination terminates or kills a job. If you display the jobs table after you press **Ctrl+Z** to suspend a job, you will see that the current job is in a suspended state (labeled in the jobs table as "Stopped"). Although the jobs table lists jobs running in the background, a foreground job that gets suspended appears in the jobs table to remind the user that there is a suspended job waiting to be restarted or terminated. Refer to the following table for a summary of job control commands.

Action	Foreground	Background
Suspend a job	Ctrl+Z	Bring to foreground, then press Ctrl+Z
Terminate a job	Ctrl+C	<code>kill %<i>n</i></code>

Restarting a Suspended Job

The `bg` command, with the syntax `bg %n`, can be used to restart a specified background job that has been suspended. You can specify the number of the suspended job you want to restart after the percent sign. If there is only one job running in the background, then you do not have to specify the number. You can type `bg %` to restart it.

Bringing a Job to the Foreground

If you need to bring a job from the background to the foreground, use the `fg` command, with the syntax `fg %n`. You do not have to enter a number after the percent sign if there is only one job running in the background.

Job Control Tools

Job control tools enable you to manipulate the jobs appearing in the jobs table.

Tool	Enables You To
<code>jobs</code>	View the status of the jobs running in the background.
Ctrl+Z	Halt a running process temporarily.
<code>fg [%job number]</code>	Bring the specified process to the foreground.
<code>bg [%job number]</code>	Send the specified process to the background.
<code>kill [%job number]</code>	Terminate the specified process.

How to Manage Jobs and Background Processes

Procedure Reference: Manage Jobs

To manage jobs:

1. Type the command with an ampersand (&) after it to put a job in the background.
2. If necessary, execute additional commands.
 - Execute another command in the background using the ampersand or;
 - Execute another command without putting it in the background.
3. To see the list of processes that are running in the background, enter `jobs` at the command line.
4. Manage the jobs that are running in the background.
 - To kill a process in the background, enter `kill [%job number]`.
 - To switch a background process to the foreground, enter `fg [%job number]`.
 - To suspend a foreground job, press **Ctrl+Z**.
 - To restart a suspended job, enter `bg [%job number]`.

ACTIVITY 10-1

Managing Jobs

Before You Begin:

- 1. You have logged in as root in the CLI.
- 2. The first terminal is displayed.

Scenario:

As a system administrator, you are asked to conserve the amount of time it takes to run jobs on Linux systems. You also need to manage multiple jobs instead of running one job at a time. You can accomplish this by moving jobs to be processed in the background.

What You Do	How You Do It
1. Issue three commands and place them in the background.	<ul style="list-style-type: none">a. To pause the system for 300 seconds, enter <code>sleep 300 &</code>b. To update the mlocate database, enter <code>updatedb &</code>c. To pause the system for 200 seconds, enter <code>sleep 200 &</code>d. To view the list of processes running in the background, enter <code>jobs</code>e. Verify that the three jobs are listed.
2. Terminate the last job.	<ul style="list-style-type: none">a. To kill the process that is executing the <code>sleep 200 &</code> command, enter <code>kill %3</code>b. To view the list of processes running in the background, enter <code>jobs</code>c. Verify that the status of the third job displays "Terminated," indicating that the job is terminated.

3. Bring the second job to the foreground and suspend it.
 - a. To move the job to update the mlocate database to the foreground, enter **fg %2**
 - b. To suspend the foreground job, press **Ctrl+Z**.
 - c. Verify that the status of the job is displayed as "Stopped," indicating that the job is stopped.
 - d. To restart the suspended job, enter **bg %2**
 - e. To view the list of processes running in the background, enter **jobs**
 - f. Verify that the job to update the mlocate database is running.
 - g. To clear the terminal screen, enter **clear**
-

TOPIC B

Manage Processes Using the Process Table

In the previous topic, you managed multiple processes using the jobs table. While the jobs table is unique to each user's specific shell, the process table is for the entire system. In this topic, you will manage processes using the process table.

Monitoring system processes enables system administrators to track the usage of system resources. Tracking the processes running on a system helps you manage your resource allocation better. As a Linux administrator, you will find the process table useful because it contains entries for all the processes that are started by all the users on the system. With the process table, you can manage processes on the system in a Linux environment.

The Process Table

The *process table* is a record that summarizes the current running processes on a system. It enables the administrator to keep track of all processes run by different users. Some of the details displayed in the process table include the PID, the size of the program in memory, the name of the user who owns the process, and time.

USER	PID	%CPU	%MEM	VSZ	RSS	TTY	STAT	START	TIME	COMMAND
root	2344	0.0	0.0	1656	460	tty2	Ss+	Jun29	0:00	/sbin/mingetty
root	2354	0.0	0.0	1656	432	tty3	Ss+	Jun29	0:00	/sbin/mingetty
root	2357	0.0	0.0	1656	460	tty4	Ss+	Jun29	0:00	/sbin/mingetty
root	2360	0.0	0.0	1656	432	tty5	Ss+	Jun29	0:00	/sbin/mingetty
root	2361	0.0	0.0	1656	432	tty6	Ss+	Jun29	0:00	/sbin/mingetty
root	4824	0.0	0.0	1656	432	tty1	Ss+	06:45	0:00	/sbin/mingetty
root	5252	0.4	0.9	16748	10064	tty7	Ss+	10:31	0:21	/usr/bin/Xorg :
root	5513	0.0	0.1	4920	1820	pts/1	Ss	10:49	0:00	bash
root	5654	0.0	0.0	4252	940	pts/1	R+	11:45	0:00	ps u

Figure 10-5: *The process table listing the processes running on the system.*

The Process Table vs. the Jobs Table

The process table has options that are different from the jobs table. The process table can display all processes running on the system irrespective of which user started it, including system processes started automatically at boot time. However, the jobs table shows only the processes started in a user's current shell. Also, the unique PID of processes are displayed in the process table, while the jobs table shows only their job number according to the order in which they were started. In the jobs table, only the original process is displayed as an entry, but in the process table, the original process and all subsequent processes that were started are displayed. So, a single entry in the jobs table may have more than one corresponding entry in the process table. Certain job control commands can be applied only by referring to processes by their job number.

The ps Command

The `ps` command invokes the process table. When the command is run without any option, it displays the processes run by the current shell with details such as the PID, the terminal associated with the process, the accumulated CPU time, and the command that started the process. However, different options may be used along with the command to filter the displayed fields or processes.

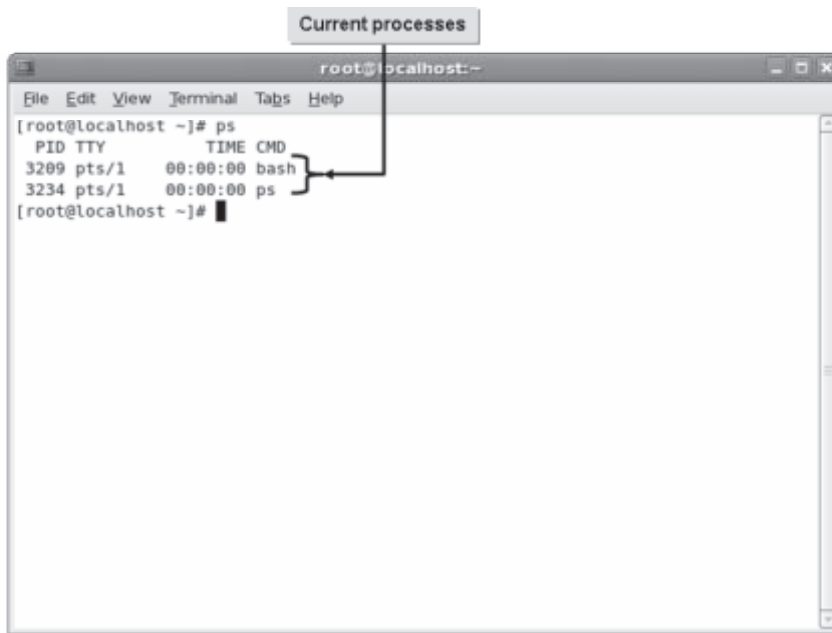


Figure 10-6: The `ps` command displaying the processes run by the current shell.

Syntax


The syntax of the `ps` command is `ps [options]`.

ps Command Options

The `ps` command supports several options.

Some of the important options are listed here.

Option	Description
<code>a</code>	Lists all user-triggered processes.
<code>-e</code>	Lists all processes.
<code>-l</code>	Lists processes using a long listing format.
<code>u</code>	Lists processes along with the user name and start time.
<code>r</code>	Excludes processes that are not running currently.
<code>x</code>	Includes processes without a terminal.
<code>T</code>	Excludes processes that were started by any terminal other than the current one.

 Unlike many commands in Linux, the `ps` command supports options with and without a hyphen before them. However, the function of the same options with or without a hyphen may differ greatly.

Command Options for Selective Display

Some common `ps` command options can be used to select a specific set of processes.

Option	Used To
<code>-U {user name}</code>	Display the processes based on the specified user.
<code>-p {PID}</code>	Display only the specified process associated with the PID.
<code>-C {command}</code>	Display all processes by command name.
<code>--tty {terminal number}</code>	Display all processes running on the specified terminal.

Fields Displayed by the ps Command

Various options display different fields. Several fields can be displayed using the `ps` command.

Field	Description
PRI	Process scheduling priority. Processes with low priority have higher numbers.
NI	Process nice value. Processes using less CPU time have higher numbers.
SIZE	Virtual image size.
RSS	Physical memory in KB.
WCHAN	Kernel function in which the process resides.
STAT	Status. Values include R (running), T (stopped), D (asleep and uninterruptible), S (asleep), Z (zombie), and N (positive nice value).
TT	The TTY or terminal associated with the process.
PAGEIN	The number of major page faults.
TRS	Resident text size.
SWAP	Number of KB of swap used.
SHARE	Amount of shared memory.

Child Processes

A process created by a running process is called a *child process*. The process table contains both *parent processes* and child processes. There may be several levels of processes. The parent process can spawn a child process, the child process can spawn another child process, and so on. The parent process must be running for the child processes to run. Parent processes are assigned a unique *Parent Process ID (PPID)*.



Figure 10-7: The process tree showing parent and child processes.

Identifying Child Processes

Identifying child processes is not an easy task, especially if there are multiple processes and child processes running at the same time. By examining the order of the PIDs, you may be able to determine the order in which the processes were created and infer which processes are related.

The `pstree` Command

The `pstree` command enables you to list the processes running on a Linux system in a tree-like format. This helps you track parent and child processes. All processes are listed as child processes to `init` and this is represented by the initial branching. The processes started within a shell will branch out of the shell's parent process.



Figure 10-8: The *pstree* command displaying parent and child processes.

Process Identification Commands

Process identification commands enable you to extract information about a process using its name or some other attributes associated with it.

Command	Description
pidof	Displays the PID of the process whose name is specified and can be used only when the name of the process is known. However, it is recommended that a full path name of the process be given because more than one process could run with the same name. The syntax of this command is <code>pidof [options] {string}</code> .
pgrep	Displays the PID of processes that match any given criteria such as the name or UID of the user who invoked it, the start time, the parent PID, and so on. The syntax of this command is <code>pgrep [options] {process name}</code> .

pidof Command Options

The `pidof` command supports only two options.

Option	Used To
-s	Instruct the program to display only one PID.
-c	Instruct the program to display the PIDs that are running from the same root directory.

pgrep Command Options

The `pgrep` command supports different options by which one or more conditions for search may be specified.

Option	Used To
-f	Specify the full path name of the process.
-l	Print the name of the process along with its PID.
-u {userid}	Specify the UID of the user who started it.
-G {groupid}	Specify the GID related to the process.
-n	Specify the most recent process.
-o	Specify the oldest process.

Signals

Definition:

Signals are messages sent to a process to perform certain actions. They are used to suspend or terminate processes. Signals may affect only the process specified and its child processes. Signals may be executed, caught, blocked, or ignored by processes.

Example:

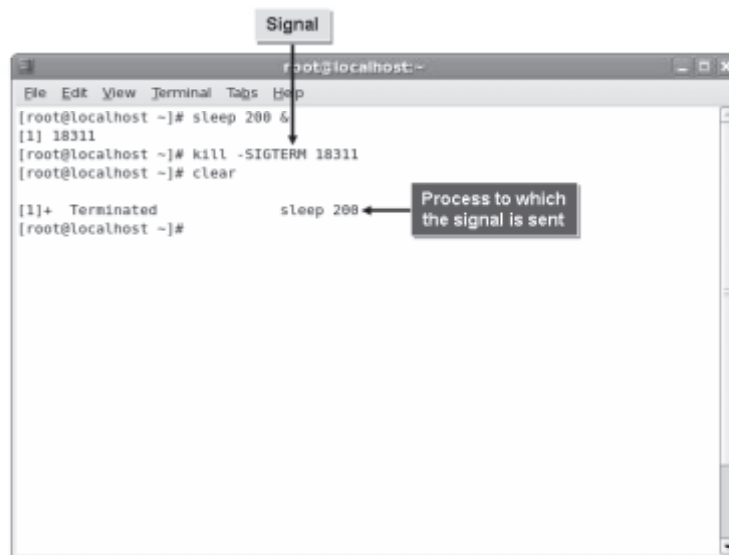


Figure 10-9: A signal sent to a process.

kill Commands

Different commands are used to send signals to processes to end or “kill” them.

Command	Description
<code>kill</code>	Sends any specified signal, or by default the termination signal, to one or more processes. The PID must be specified as the argument. The syntax of this command is <code>kill [options] {PID}</code> .
<code>pkill</code>	Signals processes based on the name and other identifiers as in the <code>pgrep</code> command. The syntax of this command is <code>pkill [options] {command}</code> .
<code>killall</code>	Kills all processes by the name specified. The syntax of this command is <code>killall [options] {command}</code> .



The `kill` command accepts either the PID or the job number as an argument. So, this command can also be used as a job control tool.

Kill Signal Options

You can either use the kill signal option or its corresponding numerical value to send a signal to terminate a process. The following table lists the most frequently used kill signal options and their description.

Option	Used To
<code>SIGKILL</code> or 9	Send the kill signal to a process.
<code>SIGTERM</code> or 15	Send the termination signal to a process.
<code>SIGSTOP</code> or 19	Stop a process.



Sometimes, even after closing an X session, some of the X applications may not get terminated properly. In such cases, you need to use the `ps` command to identify the PID of that application and then kill the process.

Using the PID Number to Terminate Processes

You can use the `kill` command with the process table to end processes. By entering `kill` followed by the PID, you can terminate specific processes.

When you use the `kill` command with the jobs table, you are working only with the jobs that you started. However, the process table may display processes that do not belong to you. As a user, you can use the `kill` command only with processes that you own. As root, you can kill anyone's processes.

There are many options available with the `kill` command. These options are referred to as kill signals. Some processes cannot be eliminated by the `kill` command. To terminate these processes, use the `kill` command with the `-9` signal. This terminates the processes immediately.

Process States

A process state enables you to identify the current stage of a process. It is indicated by a single letter notation in the process table.

The various process states are given in the table below.

State	Description
Uninterruptible sleep (D)	The process is permanently inactive.
Running (R)	The process may be running or ready to be run.
Interruptible sleep (S)	The process is waiting to be run after some specific trigger.
Stopped (T)	The process may be temporarily stopped by a job control tool or because it is being traced.
Dead (X)	The process has been killed. This state is never displayed.
Defunct (Z)	The process has ended, but only after its parent process. This implies that it has not been killed properly and it will remain as a “zombie.”

The top Command

The `top` command lists all tasks running on a Linux system. It acts as a process management tool by allowing users to prioritize, sort, or terminate processes interactively. It displays a dynamic process status, reflecting real-time changes. Different keystrokes within this tool execute process management actions.

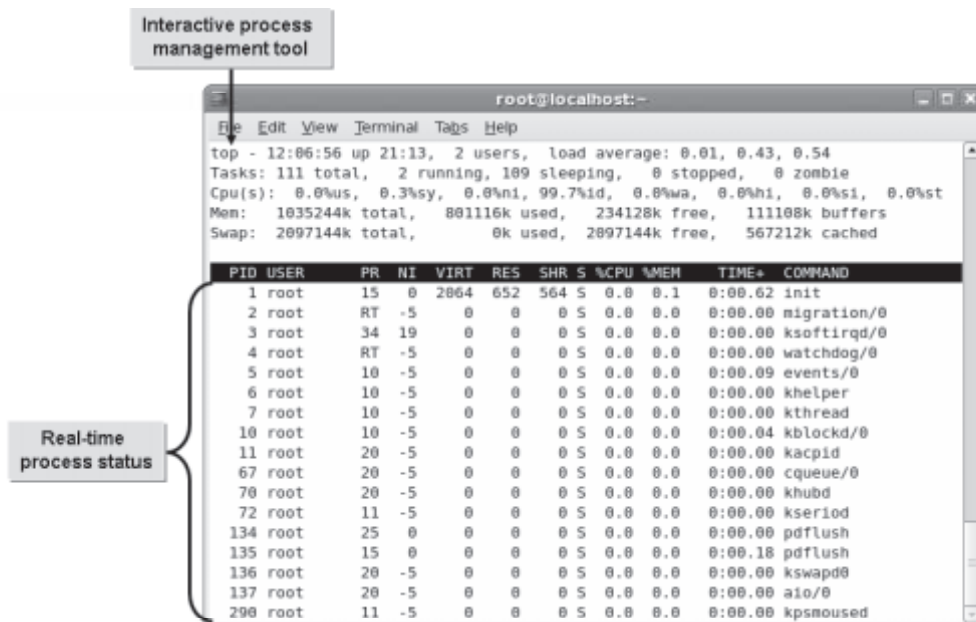


Figure 10-10: Managing processes using the `top` command.

Useful Keys to Manage Processes

The `top` command provides an interactive tool to manage processes by using some simple shortcuts. Some of the frequently used shortcuts are listed here.

Key	Function
Enter	Refreshes the status of all processes.
Shift+n	Sorts tasks in the decreasing order of their PID.
u	Displays processes belonging to the user specified at the prompt.
k	Terminates the process for which you specify the PID.
r	Renices the process for which you specify the PID.
h	Displays a help screen.
q	Exits the task list.

The nice Command

The *nice* command allows you to assign a priority level to a process. The nice value of a process indicates how “nice” the process is to others in sharing system resources. You can run a command at a priority higher or lower than the command’s normal priority. You must have the root user authority to run a command at a higher priority. The priority of a process is often called its *nice value*.

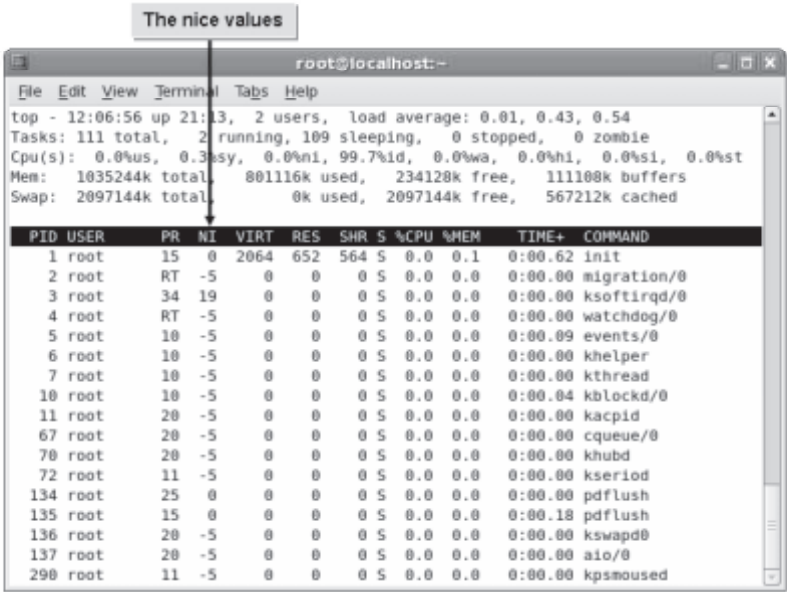


Figure 10-11: The nice values of processes running on a system.

Syntax

The syntax of the command is `nice -n {priority} {command}`, where the priority is specified by a number.

Nice Values of Processes

The niceness of a process may range from -20 to 19, where -20 indicates the highest priority and 19 the lowest. In the absence of an increment value, the `nice` command assumes an increment of 10 by default. Once lowered, the priority for any process cannot be increased by normal users, even if they own the process. By default, all processes in Linux have a nice value of zero.

The `renice` Command

The `renice` command enables you to alter the scheduling priority of a running process. When you `renice` a process group, it causes all processes in the process group to have their scheduling priority altered. When you `renice` a user, it alters the scheduling priority of all processes owned by the user. By default, the processes affected are specified by their PIDs.



Figure 10-12: Changing the priority of a process using the `renice` command.

Syntax

The syntax of the `renice` command is: `renice {priority} {PID} [[-g] [groupid]] [[-u] [userid]]`.

The GNOME System Monitor

The GNOME system monitor is an effective process management tool in the GUI. It provides a real-time display of all processes running on your system, and allows you to halt, resume, terminate, or `renice` any process. In addition to managing processes, the application also allows you to track system resources such as CPU and memory usage. It also displays details on filesystem allocation and the disk space used.

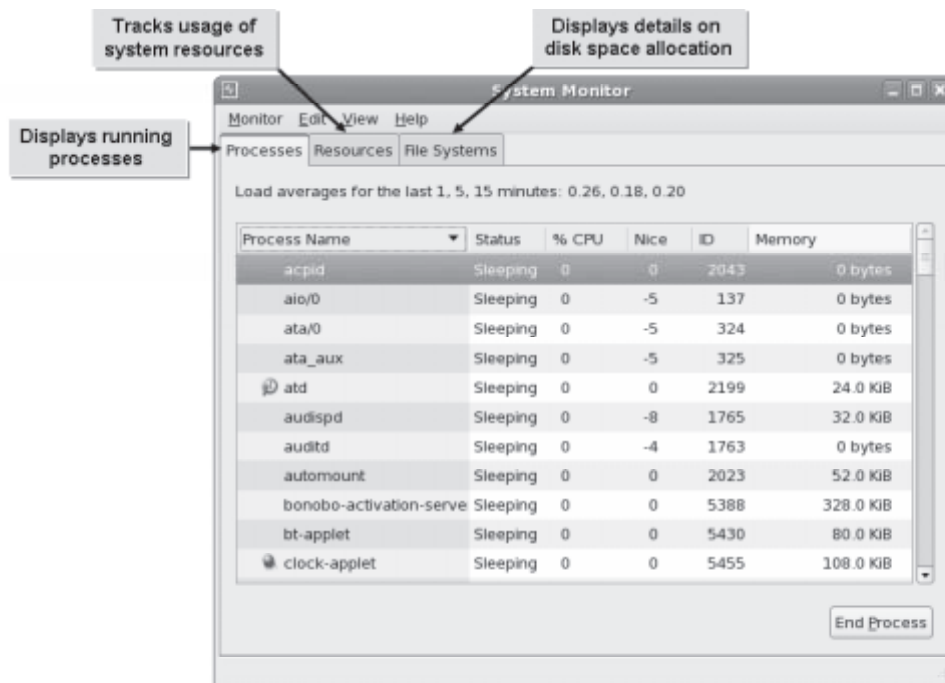


Figure 10-13: Managing processes using the GNOME system monitor.

How to Manage Processes Using the Process Table

Procedure Reference: Manage Processes

To manage processes:

1. Log in as root.
2. Manage the processes on the system.
 - To view the processes running from the current table, enter `ps`.
 - To view all processes running on the system, enter `ps -e`.
 - To terminate a process, enter `kill [PID]`.
 - To terminate a process unconditionally, enter `kill -9 [PID]`.

Procedure Reference: Change the Priority of a Process

To change the priority of a process:

1. Log in as root.
2. Change the priority of a process as necessary.
 - To start the process with the specified priority, at the command prompt, enter `nice -n {priority} {command}`.
 - To change the priority of a running process with a specified priority, enter `renice {priority} [options]`.

Procedure Reference: Change the Priority of a Process Using the top Command

To change the priority of a process using the `top` command:

1. Log in as root.
2. To display processes sorted according to their CPU usage, enter `top`.
3. To alter the priority of a particular process, press **R**.
4. Enter the PID of the process for which you want to change the priority.
5. Enter the priority number.
6. To quit the display, press **Q**.

Procedure Reference: Manage Processes Using the GNOME System Monitor

To manage processes using the GNOME system monitor:

1. Log in as root in the GUI.
2. Open the System Monitor window.
 - In the terminal window, enter `gnome-system-monitor` or;
 - In **GNOME Panel**, choose **System**→**Administration**→**System Monitor**.
3. To locate the process, on the **Processes** tab, scroll down or up.
4. To start, stop, kill, or change the priority, right-click a running process and choose the relevant option.
5. To close the window, choose **Monitor**→**Quit**.

ACTIVITY 10-2

Managing Processes

Before You Begin:

1. You have logged in as root in the CLI.
2. The first terminal is displayed.

Scenario:

Some users complained of processes on the Linux server taking longer than normal to complete. You discover several processes that are not needed are still running and were never successfully terminated. You need to manage the system processes and the processes issued by other users.

LESSON 10

What You Do	How You Do It
1. View the current running processes and all other running processes.	<ol style="list-style-type: none">To list only the processes running on the current terminal, enter psObserve that only some processes are listed.To list all the processes running on the system, enter ps -eObserve that more processes are listed as compared to the output of the ps command.
2. Issue a command.	<ol style="list-style-type: none">To pause the system for 300 seconds, enter sleep 300 &Observe the PID of the sleep 300 & command.To list only the processes running on the current terminal, enter psObserve that the sleep command is in the list of running processes.
3. Terminate the command.	<ol style="list-style-type: none">To terminate the process running the sleep command, enter the PID noted earlier in the format kill [PID]To list only the processes running on the current terminal, enter psObserve that the sleep command is not in the list of running processes and its status is displayed as "Terminated."To clear the terminal screen, enter clear

ACTIVITY 10-3

Prioritizing Processes

Before You Begin:

You have logged in as root in the CLI. The first terminal is displayed.

Scenario:

You want to back up the local copy of your installation CDs. You expect the copying process to be time consuming and to continue after you log out of your system. You decide to increase the priority of the process to ensure that it is completed on time and to allow the process to continue even after you log out.

What You Do	How You Do It
1. View the processes on your system.	<ol style="list-style-type: none"> To view all processes run by users, enter ps xl less Examine the processes that have the highest nice value. To view the next page of the list, press Page Down. Press Page Down until you reach the end of the entire list. To exit the list, press Q. Clear the terminal screen.
2. Issue the command to copy the installation files as a background process.	<ol style="list-style-type: none"> To begin the copy process, enter cp -r /rhelsource/Server /opt/. & <div data-bbox="755 1327 799 1375" data-label="Image"></div> <p>The period (.) is also part of the code. Ensure that you include it while performing this step.</p> Observe that the PID and the job number are displayed.

3. Renice the copy process by using the `top` command.
 - a. To open the process management tool, enter `top`
 - b. To renice the process, press `R`.
 - c. To specify a process to renice, enter `{PID}`
 - d. To specify the nice value, enter `-15`
 - e. To exit the process list, press `Q`.
 - f. To view the files in the Server directory, enter `ls /opt/Server`
 - g. Observe that the files from the source CD are listed, which indicates that the copy process is successful. Clear the terminal screen.

TOPIC C

Examine Delayed and Detached Jobs

You now have a basic understanding of managing jobs and processes. At times of high CPU usage, you may have to delay or stop some jobs in order to complete jobs of higher priority at a faster pace. In this topic, you will delay and detach jobs.

Some jobs can make use of a lot of system resources, and you may want to run these jobs when the system is less busy—for instance, during evening hours. Linux allows you to delay and even detach jobs, facilitating efficient utilization of system resources.

Delayed and Detached Jobs

Delayed and detached jobs are job processes that enable users to put off the start of a job.

Process	Definition
Delay a job	A <i>delayed job</i> is one that can be run at some specified time after you issue the command. For example, a CPU-intensive job that can slow down the system is one that you may want to delay for off-peak work hours.

Process	Definition
Detach a job	A <i>detached job</i> is a job that can be set to run after you log out of the system. For example, a task that will not be completed until after you leave can be set to continue running after you log out of the system.

Delaying the Start of a Process

To delay the start of a job, use the `sleep` command followed by the delay in seconds and the command name. The `sleep` command suspends any action upon the specified command for the specified number of seconds and then the command specified is executed. The delay can be up to 2,147,483,647 seconds. This is roughly 596,523 hours; 24,855 days; or 68 years so that the amount of time can easily be customized.

The nohup Command

The `nohup` (no hangup) command tells a program to ignore the hangup signal that was sent while disconnecting. The `nohup.out` file stores the output of the `nohup` command, which will normally be displayed on the terminal.

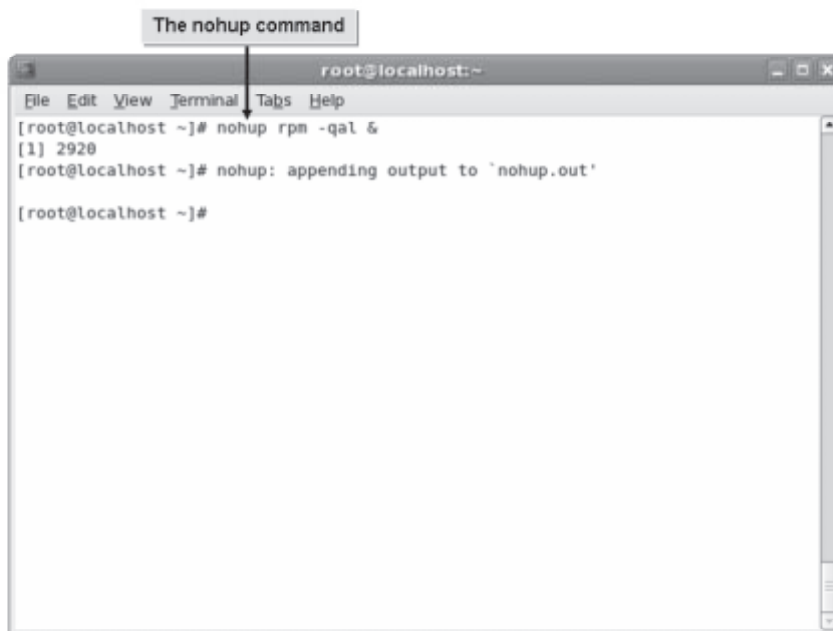


Figure 10-14: Enabling a background process to run after logging out of the system using the `nohup` command.

Running a Process After You Leave the System

If you have a task that cannot be completed until after you leave work, or if you have a task that is CPU intensive and may slow the system, you can start the task before you leave and specify that it continues even after you log out of the system. You can do this by using the `nohup` (no hangup) command. The `nohup` command should run in the background so that it does not tie up your terminal. To enable a command to run in the background after you have logged out, use the syntax `nohup [command] &`.

How to Work with Delayed and Detached Jobs

Procedure Reference: Delay a Job

To delay a job:

1. Log in as root.
2. Determine the job that you want to schedule later. To schedule the job at a later time, enter `sleep {number of seconds to delay} [command to issue]`.

Procedure Reference: Detach a Job

To detach a job:

1. Log in as root.
2. Determine the job that you want to run after you log out of the system. To schedule the job to continue running even after you log out, enter `nohup {command to issue} &`.

ACTIVITY 10-4

Detaching a Job

Before You Begin:

1. You have logged in as root in the CLI. The first terminal is displayed.
2. To view the running processes, on the terminal, enter `ps`.
3. In the **CMD** column, note the PID of the `cp` process.
4. To kill the `cp` process, enter `kill {PID}`.
5. To clear the terminal screen, enter `clear`.

Scenario:

You discovered that a large number of CPU-intensive jobs are being run during the normal business hours. Your manager gave you a list of jobs that are not time critical and can be rescheduled. You decide that the best time to run CPU-intensive applications is after you log out of the system.

What You Do	How You Do It
1. Issue a command to run in the background and log out.	<ol style="list-style-type: none"> To view the files that are available in the <code>/etc</code> directory, on the terminal, enter find /etc Observe that the <code>/etc/sysctl.conf</code> file is the last entry in the <code>/etc</code> directory. To process the command in the background, enter nohup find /etc -print & and to continue, press Enter. Observe that a message is displayed indicating that the output of the command is added to the <code>nohup.out</code> file. Enter logout
2. Log in as root and verify that the job is complete.	<ol style="list-style-type: none"> At the login prompt, enter root At the Password prompt, enter p@ssw0rd To open the <code>nohup.out</code> file, enter vim nohup.out Observe that the file contains a listing of files and directories in the <code>/etc</code> directory, which indicates that the job is complete. To move to the end of the file, press Shift+G. Observe that the <code>/etc/sysctl.conf</code> file is the last entry listed. Type : in command mode. To close the file, enter q To clear the terminal, enter clear

TOPIC D

Schedule Jobs

In the last topic, you delayed and detached jobs to overcome high CPU usage. You may also need to designate jobs that are to be executed at a specific time. In this topic, you will schedule jobs.

As a system administrator, you may need to schedule repetitive tasks to run at a specific time. For example, you may schedule a backup process every night so that it does not affect the work schedule of the users. Scheduling jobs is an important part of a system administrator's daily tasks.

Cron

Definition:

Cron is a daemon that runs in the background on a Linux system and executes specified tasks at a designated time or date. Cron is normally used to schedule periodically executed tasks defined in the *crontab* file.

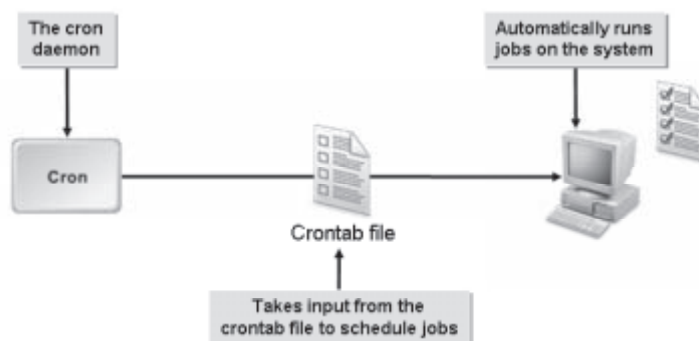
Example:

Figure 10-15: *Cron executes specified tasks on the system.*

Syntax

The syntax of the cron daemon is `cron [option] {mail command}`.

Significance of the /etc/cron Directories

Under the /etc directory, you will find directories such as `cron.d`, `cron.hourly`, `cron.daily`, `cron.weekly`, and `cron.monthly`. Depending on the frequency of the execution of bash script, you need to place your script file in the `cron.hourly`, `cron.daily`, `cron.weekly`, or `cron.monthly` directory. If you want to run a shell script for a frequency other than hourly, daily, weekly, or monthly, you need to place the script in the `cron.d` directory.

Cron Jobs

A task scheduled via cron is called a *cron job*. These jobs will run either at system level or at user level. The cron jobs that you create for users are stored in the `/var/spool/cron/[user name]` file. System default cron jobs are stored in the `/etc/crontab` file. Only a root user can add system level jobs.

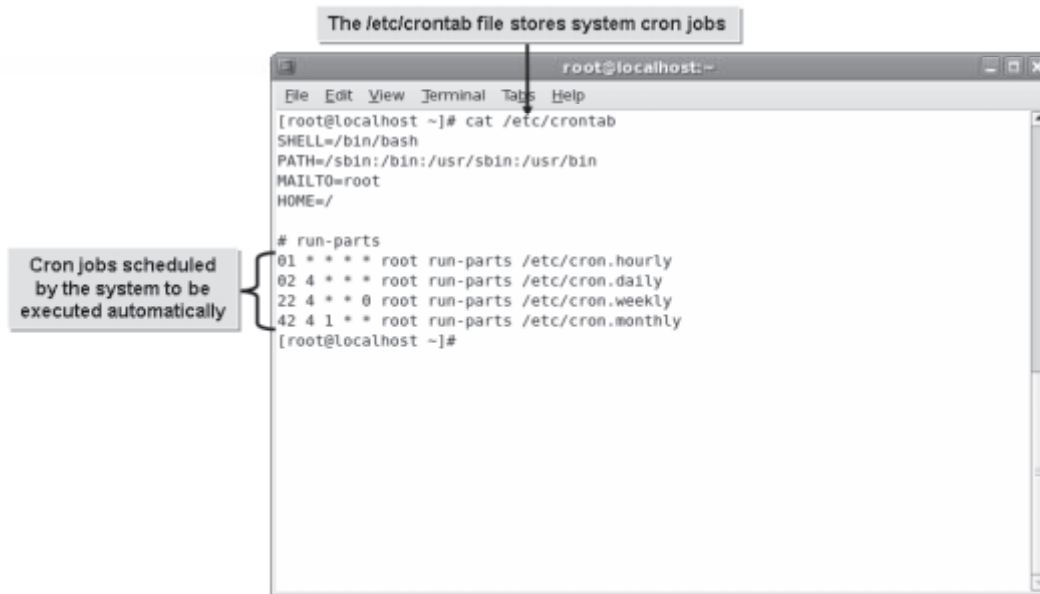


Figure 10-16: Cron jobs listed in the crontab file.

Setting Up Scheduled Jobs Using cron

Scheduling a cron job is accomplished by adding the job to the system-wide `/etc/crontab` file. The crontab file may also contain environment variables that will be passed to the commands at the time of execution. Jobs in the crontab file are called entries, and they include a time description, the user name to run the command, and the command. The format of a crontab entry is: `{minute} {hour} {day of month} {month} {day of week} {user command}`. The time fields in the crontab entry are listed here.

Field	Allowed Value
Minute	0-59
Hour	0-23
Day of the month	1-31
Month	1-12 or Jan-Dec
Day of the week	0-7 (0 or 7 is Sunday) or Sun-Sat

In addition to specifying a particular time and day, a pattern can be described by using asterisks (`*`) to specify all of a particular field. For example, an asterisk in the minute field indicates that the command should be carried out every minute. In addition to asterisks, time ranges are permitted by separating values with a dash (`-`) and lists of values are specified by separating values with a comma (`,`).

The tmpwatch Command

The *tmpwatch* command is run as a daily cron job that is used to delete files, such as the files in the */tmp* directory, which have not been accessed for some time and are utilizing disk space. The *tmpwatch* command has various options.

Option	Enables You To
-u	Delete files according to the time they were accessed.
-m	Delete files according to the time they were modified.
-a	Remove all file types, including directories.
-d	Restrict the <i>tmpwatch</i> command from removing directories, even if they are empty or marked for deletion.
-f	Remove files forcefully, overriding all access regulations.

 Even if one error is encountered during the cleanup process, the *tmpwatch* utility will exit.

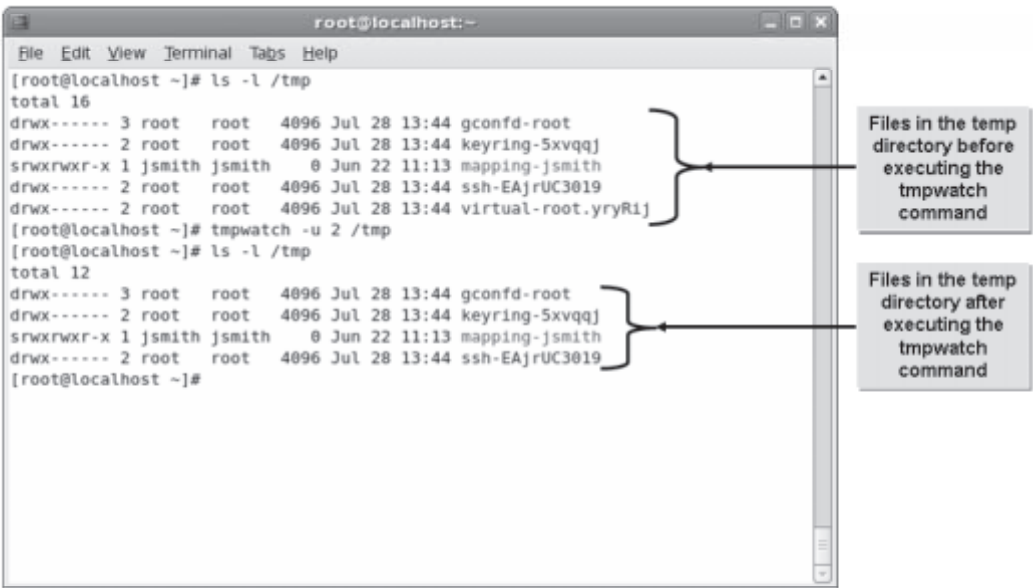



Figure 10-17: Deleting files in the */tmp* directory using the *tmpwatch* command.

Syntax

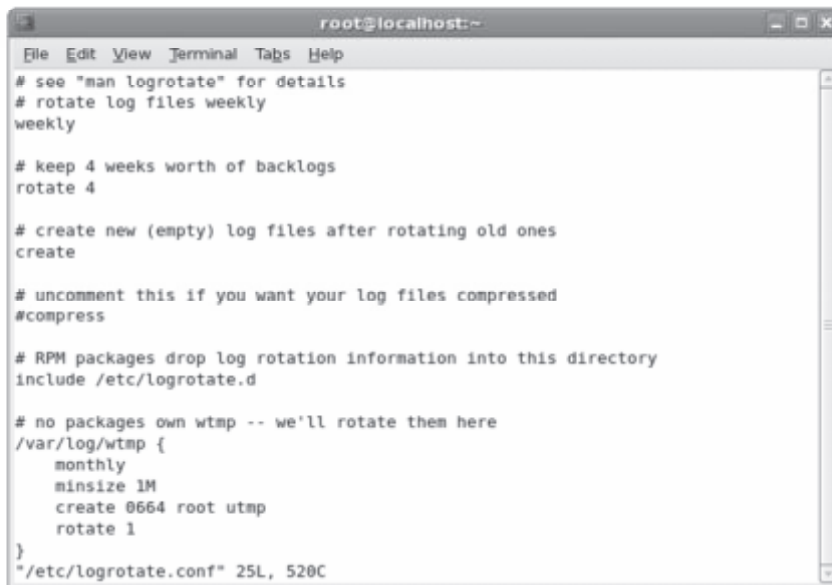
The syntax of the *tmpwatch* command is *tmpwatch [options] {hours}*.

The logrotate Command

The *logrotate* command is run as a daily cron job that is used to compress, delete, or mail log files. It may be configured to run on a weekly or monthly basis depending on the log size. The *logrotate* command has various options.

 The configuration file for `logrotate` is `/etc/logrotate.conf`.

Option	Enables You To
<code>-d</code>	Turn on debug mode to disable any change from being made to the logs.
<code>-f</code>	Force log rotation by deleting old files irrespective of their importance and create new ones.
<code>-m {subject} {recipient}</code>	Mail the logs to the recipient. The default syntax is <code>/bin/mail -s</code> .



```

root@localhost:~
File Edit View Terminal Tabs Help
# see "man logrotate" for details
# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# uncomment this if you want your log files compressed
#compress

# RPM packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own wtmp -- we'll rotate them here
/var/log/wtmp {
    monthly
    minsize 1M
    create 0664 root utmp
    rotate 1
}
"/etc/logrotate.conf" 25L, 520C

```

Figure 10-18: The `/etc/logrotate.conf` file allows you to control the rotation of logs.

The logwatch Utility

The *logwatch* utility is run as a daily cron job that is used to monitor logs. It is fully customizable via the `/etc/logwatch/conf/logwatch.conf` file. The utility searches logs and reports suspicious messages, and enables you to set detail levels for reports. 10, 5, and 0, correspond to high, medium, and low level details, respectively.

The *logwatch* utility has various options.

Option	Enables You To
<code>--detail {level}</code>	Set the detail level of the log report.
<code>--print</code>	Print the report generated by the command.
<code>--range {range}</code>	Set the range for analysis. It can accept any value among Yesterday, Today, and All.
<code>--mailto {address}</code>	Mail the results to the recipient's mail ID.

Option	Enables You To
<code>save {file name}</code>	Save the output to a file instead of displaying it.

System crontab Files

System crontab files are the configuration files for the `cron` utility. They are stored in the `/etc/crontab` file. The name of the user running the command is indicated in the sixth field of the file. When you create a crontab entry for a specific user, the sixth field contains the command that needs to be run at the specified time. System crontab files can be edited by the root user.

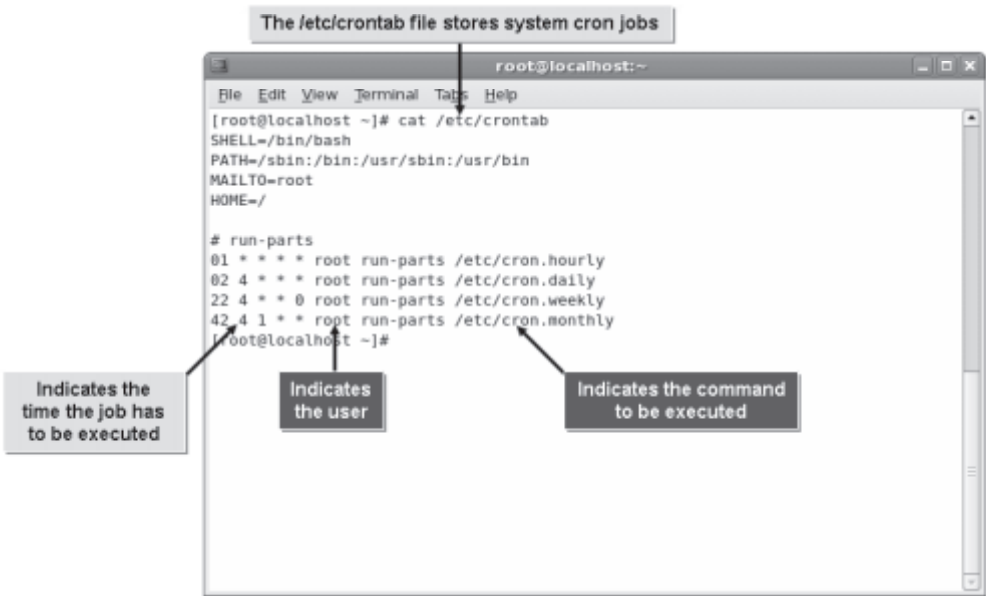


Figure 10-19: The `/etc/crontab` file with system-level cron jobs.

User crontab Files

In addition to system-level cron jobs, individual users can schedule cron jobs. Unlike the system-level crontab, users have their own crontab files. The format of entries in this file is the same as that of the system-level crontab, with the exception of the user field. Because the entire crontab file is dedicated to a single user, the user field is not included. While the `/etc/crontab` file can be edited directly, user crontab files are best edited via the `crontab` utility.

The at Command

The `at` command executes a given set of commands at a specified time. This command is useful for executing a set of commands only once. Using either the `-f` option or input redirection, the `at` command reads the list of commands from a file. This file needs to be an executable shell script.

The following table lists some frequently used `at` command options and their descriptions.

Option	Enables You To
<code>atq</code>	Display the job queue of all users except the superuser.
<code>atq -V</code>	Display the version number.
<code>at -q [a-z]</code>	Display the jobs in the specified queue.
<code>at -m</code>	Send mail to the user when the job is complete.
<code>at -f {file name}</code>	Read the job from the file rather than the standard input.
<code>at -l</code>	Print all the jobs queued for the user.
<code>at -v</code>	Display the time that the job will be executed before reading the job.

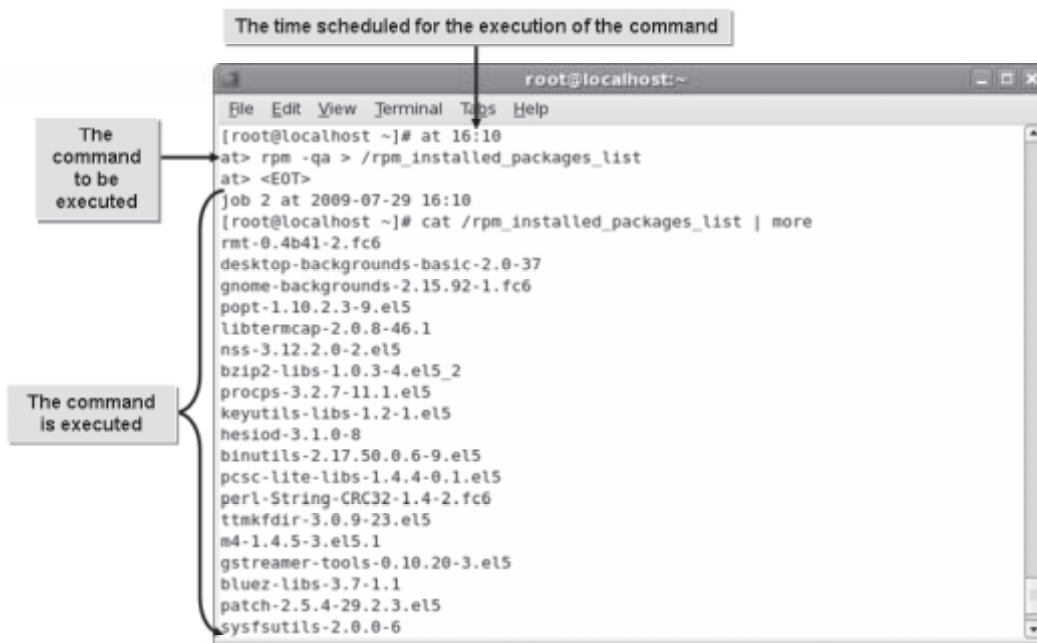


Figure 10-20: Executing a command at a specific time using the `at` command.

Syntax

The syntax of the `at` command is `at [options] {time}`.

Specifying Time Using the `at` Command

There are a number of common time formats. Some of the common time formats in which you can schedule a job are given in the following table.

Time Format	Description
HH:MM A.M. or HH:MM P.M.	Specifies the hour and minute.
MMDDYY or MM/DD/YY or DD.MM.YY	Specifies the day, month, and year.
JAN or FEB or MAR	Specifies the month.
SUN or MON or TUE	Specifies the day of the week.

Anacron

Definition:

Anacron is a daemon that executes jobs at intervals, which are specified in days, without requiring the system to be running continuously. Anacron is used to control the execution of daily, weekly, or monthly jobs.

Example:

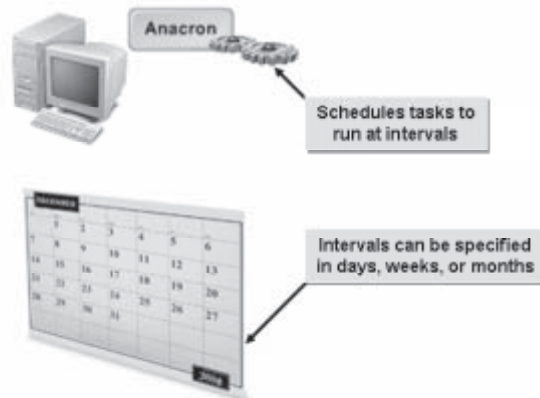


Figure 10-21: *The anacron daemon executing scheduled jobs.*

The /etc/anacrontab File

The `/etc/anacrontab` file is the configuration file for the `anacron` utility. This file has four fields. The first field displays the number of days the job has not been run, the second field displays the time after which the job has to be run (after reboot), the third field displays the job identifier, and the fourth field displays the job to be run by the `anacron` utility.

How to Schedule Jobs

Procedure Reference: Delegate Tasks Using the cron Command

To delegate tasks using the `cron` command:

1. Log in as root in the CLI.
2. To create a cron job for the root user, enter `crontab -e`.
3. To switch to input mode, press **I**.
4. To specify a schedule for the job, type `{minute} {hour} {day of month} {month} {day of week} {command that has to be run}`.
5. To install the new cron job, save and close the file.
6. To verify that the new cron job has been executed, check if you have received an email message regarding the job that has been scheduled.
7. To list the cron jobs, enter `crontab -l`.
8. To remove the job from the queue, enter `crontab -r`.

Configure Access to cron and at Services

To configure user access to `cron` and `at` services, you need to perform the following actions in the corresponding files listed in the table.

If You Need To	You Should
Allow <code>cron</code> services to users	Add users to the <code>/etc/cron.allow</code> file.
Deny <code>cron</code> services to users	Add users to the <code>/etc/cron.deny</code> file.
Allow <code>at</code> service to users	Add users to the <code>/etc/at.allow</code> file.
Deny <code>at</code> service to users	Add users to the <code>/etc/at.deny</code> file.

Procedure Reference: Schedule Jobs to Run at a Specific Time

To schedule jobs to run at a specific time:

1. Log in as root in the CLI.
2. To specify an `at` job, enter `at {specific time format}`.
3. Enter `{job that has to be run}`.
4. To exit the process, press **Ctrl+D**.
5. To verify that the `at` job has been executed, check if you have received an email message for the job that has been executed.

Procedure Reference: Manage Jobs Using the at Command

To manage jobs using the `at` command:

1. Log in as root in the CLI.
2. To view the queue of pending `at` jobs, enter `atq`.
3. To delete a job from the queue, enter `atrm {job number}`.

ACTIVITY 10-5

Scheduling Jobs Using crontab

Before You Begin:

You have logged in as root in the CLI and the first terminal is displayed.

Scenario:

Your organization adopted a new policy that requires all users to fill in their time sheets every day. The senior system administrator asked you to create a daily reminder for all user systems.

Account information for the user who needs the reminder:

- Login name: user1 and Password: myp@\$w0rd

What You Do	How You Do It
1. Schedule a cron job to email a reminder every day at a specified time.	<div>a. To create the user1 user account, enter useradd user1</div> <div>b. To set the password for user1, enter passwd user1</div> <div>c. At the New UNIX password prompt, enter myp@\$w0rd</div> <div>d. At the Retype new UNIX password prompt, enter myp@\$w0rd</div> <div>e. To view the system time, enter date</div> <div>f. To specify a cron job for user1, enter crontab -u user1 -e</div> <div>g. Observe that the text editor opens a temporary file automatically. To switch to insert mode, press I.</div> <div>h. To schedule the cron job, type ## ## * * * /bin/echo "Please fill in your time sheet"</div> <div>i. To switch to command mode, press Esc. Save and close the file.</div> <div>j. Enter logout</div>

2. Check whether user1 received the reminder for the scheduled job.
 - a. After the specified time, log in as **user1** in the CLI.
 - b. To open the mailbox, enter **mail**
 - c. To read the contents of the first email message, enter **1**
 - d. Observe that the mail contains a reminder to fill in the time sheet. To delete the email message, enter **d**
 - e. To quit the mail service, enter **q**
 - f. To log out of the **user1** account, enter **logout**
-

TOPIC E

Maintain the System Time

In the previous topic, you scheduled jobs to run at a specific time. It is not always enough to simply schedule a recurring job, however, as the system time might not be correct. You also need to monitor system clocks so that all systems show the same time. In this topic, you will maintain the system time.

Suppose you work in a company with clients in various cities around the world. You may need to synchronize your system time with that of your client's time zone to enable easier business transactions.

The NTP

Network Time Protocol (NTP) is a standard Internet protocol for synchronizing the internal system clock with the *true time* or the *average time* on a number of high accuracy clocks around the world. NTP is used for transmitting and receiving time on TCP/IP networks. NTP is also used to set the clock of one computer to match that of another and synchronize it with the network clock.

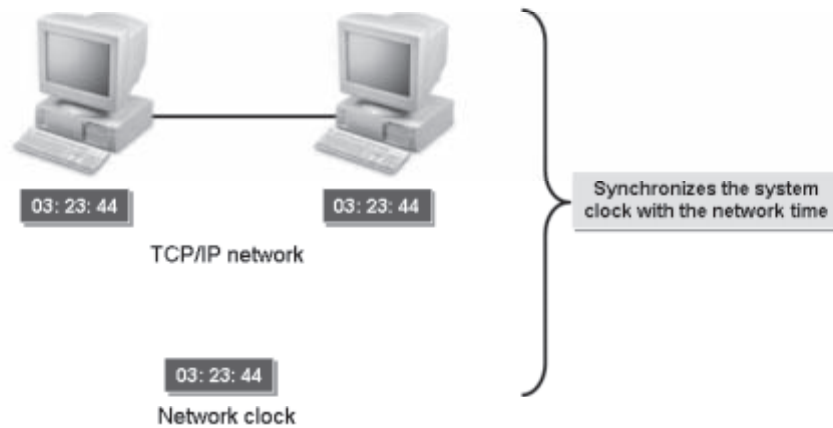


Figure 10-22: *Synchronization of system clocks with network time using NTP.*

The pool.ntp.org Service

The pool.ntp.org is a collection of servers on the Internet that provides accurate time to the Linux systems using NTP.

Drift Files

A drift file is a file found in the /etc/ntp directory. The NTP drift file is used by the ntpd daemon to reset the time when the system is restarted. The drift file synchronizes the system clock and the clock drift to display the time from the NTP server.

The ntp.conf File

The ntp.conf file found in the /etc directory contains configuration options for the NTP server. The file contains settings for all hosts on local and public servers. The ntpd daemon reads the ntp.conf file for synchronization settings and then connects to the NTP server.

UTC

Definition:

Coordinated Universal Time (UTC) is a time scale that forms the official measure of time in the world. UTC is independent of time zones. It was previously referred to as *Greenwich Mean Time (GMT)*. It is the time at the prime meridian at Greenwich, England. Unlike GMT, leap seconds are included in UTC.

Example:



Figure 10-23: World time zone.

Leap Seconds

A leap second is the adjustment made to UTC, to account for the irregularity in the earth’s rotation. The standard second is stable, while the motion of the earth is not. Therefore, occasionally, the standard minute is adjusted by adding a leap second. As a result, some minutes have 61 seconds. Standard hours are always 60 minutes, though one of the minutes may be a second longer than usual. Standard days are always 24 hours.

Linux and Time Zones

In Linux, you can use the `tzselect` command to access a menu driven utility that will allow you to select the time zone for your system according to your geographic location. You need to define an environment variable, `TZ`, in the `/etc/profile` file to set the time zone for your system.

Locale Settings

Some settings of the system vary according to the geographic location of the system. These settings are known as locale settings. Some of the common locale settings are listed in the following table.

Setting	Description
Language	The language of the system must be adjusted according to the language spoken in the country or based on the user’s choice. In Linux, you can use the <code>system-config-language</code> command to set the default language of the system.
Keyboard Layout	The keyboard layout of the system must be set according to the layout meant for inputting the language of the system. You can use the <code>system-config-keyboard</code> command to select the keyboard layout.

Setting	Description
Character Set	<p>There are different character sets or encoding methods that are available for displaying different languages. The main character sets are:</p> <ul style="list-style-type: none"> • Unicode • ISO-8859—An industry standard for 8-bit character encoding. • ASCII—A standard used for specifying numbers to represent the alphabet in both upper and lowercase. Acronym for American Standard Code for Information Interchange. • UTF-8—An encoding scheme for Unicode that allows you to handle 8-bit variable length characters. Acronym for Unicode Transformation Format. You need to use the <code>iconv</code> program to convert from one encoding format to another.
Environment Variables	<p>Some common environment variables associated with locale settings are:</p> <ul style="list-style-type: none"> • LANG—Helps in determining the local language to be used for displaying on the system and for use in system based messages. • LC_ALL—Helps in setting values for all locale settings. • LC_*—Helps in setting values specific to each locale settings. This covers the environment variables, <ul style="list-style-type: none"> • LC_COLLATE—Helps in specifying the collation of characters. Used with regular expressions and for sorting purposes. • LC_CTYPE—Helps in specifying the locale for converting casing of characters. • LC_MESSAGES—Helps in specifying the language to be used for displaying system error messages. • LC_MONETARY—Helps in specifying the currency formats for the system. • LC_NUMERIC—Helps in specifying the number formats for the system. • LC_TIME—Helps in specifying the date and time formats for the system.

The /usr/bin/locale File

The `/usr/bin/locale` file is an executable program that prints the current value of the locale settings on the standard output device. It displays the current value set for the locale variables such as `LANG`, `LC_CTYPE`, `LC_NUMERIC`, `LC_TIME`, `LC_COLLATE`, `LC_MONETARY`, `LC_MESSAGES`, and `LC_ALL`.

Clock Drift

Clock drift is the gradual variation in time that sets between the hardware clock and the system clock. The hardware clock is also known as the *Real Time Clock (RTC)*. It keeps track of the time when the system is turned off and not when the system is on. The system clock, however, functions only when the system is running and needs to be initialized at boot time. The hardware and system clocks will drift at different rates, apart from each other and also away from the real time. To synchronize both clocks, their drift rates need to be measured and corrected.

System Time

Definition:

System time is the time maintained by a computer's internal clock. It is coordinated universal time with a resolution in milliseconds. The internal clock circuitry is backed up by a battery that keeps the clock running even when the computer is switched off. System time is used to date-stamp files with the time of their creation or revision. It can also be changed with difference in time zones.

Example:



Figure 10-24: System time on the GNOME desktop.

The system-config-date Command

The `system-config-date` command allows you to open the **Date/Time Properties** dialog box that facilitates changing the system date and time and configuring the time zone.

The Date/Time Format

The International Organization for Standardization (ISO) specifies numeric representation of date and time. The standard format for date is YYYY-MM-DD, where YYYY represents the year in the Gregorian calendar, MM represents the month in the year, and DD represents the day in the month. The American format of date is MM-DD-YYYY. However, Europeans write the day before the month. The separators used with numbers also vary among countries. The common format for time is hh-mm-ss, where hh represents hours, mm represents minutes, and ss represents seconds.

How to Maintain the System Time

Procedure Reference: Synchronize the System Clock with the Remote Time Server Using the `system-config-date` Command

To synchronize the system clock with the remote time server using the `system-config-date` command:

1. Log in as root in the GUI.
2. Open the Date/Time Properties window.
 - In **GNOME Panel**, choose **System**→**Administration**→**Date & Time** or;
 - On the terminal, enter the `system-config-date` command.
3. Select the **Network Time Protocol** tab.
4. Synchronize the system clock with the remote time server using NTP.
 - a. Check the **Enable Network Time Protocol** check box.
 - b. Add a new NTP server.
 1. To add the NTP server, click **Add**.
 2. To add the new server to the **NTP Servers** list, in the **New NTP Server** text box, enter the domain name of the NTP server in the format `{server name}.pool.ntp.org` or specify a desired domain name.
 3. If necessary, to discard the NTP server entry, in the message box with the message “**Host {ntp server} is not reachable or doesn’t act as an NTP server,**” click **No**.
 - c. Manage the existing NTP server list.
 - To edit the existing entry, select the entry and click **Edit**.
 - To delete the existing entry, select the entry and click **Delete**.
 - d. If necessary, to use the hidden advanced options, click the **Show advanced options** button.
 - Check or uncheck the **Synchronize system clock before starting service** check box.
 - Check or uncheck the **Use Local Time Source** check box.
5. To apply the settings and close the window, click **OK**.

Procedure Reference: Synchronize the System Clock with the Remote Time Server Using the `/etc/ntp.conf` File

To synchronize the system clock with the remote time server using the `/etc/ntp.conf` file:

1. Log in as root.
2. To navigate to the `/etc` directory, enter `cd /etc`.
3. To open the `ntp.conf` file, enter `vi ntp.conf`.
4. Specify the time server details.
 - To set the server details, enter `server { ip-address | FQDN of the time server }`.
 - To set the drift file location, enter `drift file { drift file location }`.
5. Save and close the file.
6. To manually reset the clock, enter `ntpdate`.
7. To display a list and summary of the NTP servers known to the server, enter `ntpq -p`.



`ntpq` is a utility that is used to monitor the `ntpd` service and determine its performance.

Procedure Reference: Set the System Date and Time

To set the system date and time:

1. Log in as root in the CLI.
2. Enter `date [MMDDHHmm] [[CC] [YY] [.ss]`, where MM indicates the month, DD indicates the date, HH indicates the hour, mm indicates the minute, CC refers to the century part of the year, YY refers to the year, and ss refers to the seconds. For example, 10111555 indicates October 11th 3:55 P.M.

Procedure Reference: Configure the Correct Time Zone for the System

To configure the correct time zone for the system:

1. Log in as root in the CLI.
2. If desired, to view the current time zone, enter `date`.
3. To start the menu-driven time zone selection process, enter `tzselect`.
4. Enter the number corresponding to the continent or ocean.
5. Enter the number corresponding to the country.
6. If necessary, for countries with multiple time zones, enter the number corresponding to the time zone.
7. To accept the settings, enter `I`.
8. Apply the changes.
 - a. To view the value of the TZ variable, make a note of the line `TZ='{Continent/City}'`; and export TZ.
 - b. Enter `vi /etc/profile`.

- c. In a new line, enter `TZ= '{Continent/City}'`.
 - d. To export the variable, type `export TZ`.
 - e. Save and close the file.
9. To view the changed settings, log out and log in.

The /etc/timezone File

The `/etc/timezone` file is available with the Debian distribution of Linux and is used to store the time zone information of the system. This file typically consists of a single line entry based on the continent/time zone format, such as `America/New_York`.

The /usr/share/zoneinfo/ Directory

The `/usr/share/zoneinfo/` directory contains time zone details relating to different countries. When you export a time zone, details of that time zone are obtained from this directory.

The /etc/localtime Directory

The current time details of the system are stored in the `/etc/localtime` directory. If you make any change to your system time, the `/etc/localtime` directory gets updated.

The tzconfig Utility

The `tzconfig` utility allows you to set the time zone for Debian Linux. When you run this utility it will update the time zone in the `/etc/timezone` file and the files in the `/etc/localtime` directory.

Procedure Reference: Set the BIOS Clock to the Correct Time in UTC

To set the BIOS clock to match the correct time in UTC:

1. Log in as root in the CLI.
2. To verify the UTC for your time zone, enter `date --utc`.
3. Set the BIOS clock.
 - Enter `hwclock --set --date='YYYY-MM-DD hh:mm:ss'` or;
 - Enter `hwclock --utc`.

hwclock Command Options

The `hwclock` command is used to access the hardware clock. The `hwclock` command consists of various options.

If You Need To	Use This <code>hwclock</code> Command Option
Set the BIOS clock to the time given by <code>--date</code> .	<code>--set</code>
Specify the time that will be set for the BIOS clock.	<code>--date=[YYYY-MM-DD hh:mm:ss]'</code>
Set the system time from the BIOS clock.	<code>--hctosys</code>
Set the BIOS clock from the system time.	<code>--systohc</code>
Set the BIOS clock to the UTC.	<code>--utc</code>

Procedure Reference: Synchronize the Clock over NTP

To synchronize the clock over NTP:

1. Log in as root in the CLI.
2. Configure the NTP client.
 - a. Enter `vi /etc/ntp.conf`.
 - b. To specify the NTP server, enter `server {FQDN of the NTP server}`. If you have multiple NTP servers, specify the server address in sequence.
 - c. To synchronize with the NTP server, enter `restrict {FQDN of the NTP server} mask 255.255.255.255 nomodify notrap noquery`.
 - d. Save and close the file.
 - e. To start the NTP service, enter `service ntpd start`.
 - f. If necessary, to specify the drift in the time, edit the `/var/lib/ntp/drift` NTP drift file.



The `ntpd` daemon is used to synchronize the system time with the NTP server.

The ntpdate Command

When the `ntpd` daemon is not running, you can use the `ntpdate` command to manually synchronize your system time with the NTP server. For example, `ntpdate -s {FQDN of the NTP server}`.

ACTIVITY 10-6

Synchronizing System Clocks**Before You Begin:**

1. The login screen of the first terminal in the CLI is displayed.
2. Switch to the GUI.
3. You have logged in as root in the GUI.
4. The terminal window is displayed.

Scenario:

In the company where you work as a system administrator, all employees are required to fill in their time cards, to keep track of their daily duties. You are assigned the task of standardizing the time displayed on all systems, to ensure that all users enter the correct time in their time cards. As part of the auditing task, you want to ensure that all systems on the network have their time synchronized to the time server. To ensure uniformity in the time cards, you decide to configure NTP.

LESSON 10

What You Do	How You Do It
1. Open the ntp.conf file.	<ol style="list-style-type: none">To navigate to the /etc directory, enter cd /etcTo open the ntp.conf file, enter vi ntp.conf
2. Synchronize the system time with the server.	<ol style="list-style-type: none">To go to the last line of the file, press Shift+G.To switch to insert mode and move to a new line, press O.On the new line, type <i>server {IP address of server}</i>To switch to command mode, press Esc.Save and close the file.
3. Enable NTP.	<ol style="list-style-type: none">To open the Date/Time Properties window, enter system-config-dateSelect the Network Time Protocol tab.To synchronize the system clock with the remote time server using NTP, check the Enable Network Time Protocol check box.Verify that the NTP servers from the pool.ntp.org domain are displayed.To apply the settings and close the window, click OK.Observe that a message "Contacting NTP server" is displayed.Clear the terminal window.

ACTIVITY 10-7

Configuring the System Time Zone

Before You Begin:

- 1. You have logged in as root in the GUI.
- 2. The terminal window is displayed.
- 3. Switch to the CLI.
- 4. Log in as root.

Scenario:

Your organization has a 24x7 help desk that provides continuous support to clients around the world. One of the help desk executives is instructed to have her system time synchronized with that of the Japanese Standard Time zone (JST) so that she can service Japanese clients.

What You Do	How You Do It
1. Change the time zone.	<ul style="list-style-type: none">a. To view the present time zone, enter dateb. Observe that the current time zone of the system is "EDT."c. To start the menu-driven time zone selection process, enter tzselectd. To select Asia as the continent, enter 5e. To select Japan as the country, enter 19f. To accept the settings, enter 1

LESSON 10

2. Apply the changes.
 - a. Enter **vi /etc/profile**
 - b. To define the **TZ** variable, on a new line, type **TZ='Asia/Tokyo'** and press **Enter**.
 - c. To export the **TZ** variable, type **export TZ**
 - d. Press **Esc**.
 - e. Save and close the file.
 - f. Enter **logout**
 - g. To apply the settings, log in as **root**
 - h. To view the changed time zone setting, enter **date**
 - i. Observe that the new time zone of the system is "JST."
 - j. Enter **logout**
-

Lesson 10 Follow-up

In this lesson, you managed essential jobs and processes on a Linux system. This will enable you to effectively track the usage of system resources and manage resource allocation efficiently.

1. How can a system's performance be improved by managing processes?
2. Do you think automating system processes affect a system's performance? Why?

LESSON 11

Managing System Services

Lesson Time*1 hour(s), 30 minutes*

In this lesson, you will manage system services.

You will:

- Configure system services to improve system performance.
- Monitor system logs.
- Configure SELinux.

Introduction

Now that you examined the way processes operate in a Linux environment, you can manage the services that run on a Linux system. These include basic services and other services that are required by the kernel to process requests. In this lesson, you will manage system services.

With system services, you can make various system resources available to different users. At times, you may need to start, stop, or restart services to keep a system running efficiently. By managing system services, you can ensure that the system is working at the optimum level and users are able to derive maximum benefits.

This lesson covers all or part of the following CompTIA Linux+ Powered by LPI certification objectives:

- Topic A:
 - Objective 101.3, Objective 110.2
- Topic B:
 - Objective 101.2, Objective 103.2, Objective 103.7, Objective 108.2

TOPIC A

Configure System Services

On a Linux system, there are numerous services that will be running simultaneously. These services need to be secured and managed properly in an efficient manner to avoid any clogging of system resources. In this topic, you will configure system services.

As a Linux administrator, you will often face performance problems, such as slow processing and improper system response, with your system. Often, these problems are a result of improperly managed services that utilize more system resources, causing other processes to run on minimal resources. By managing system services properly, you will be able to increase the efficiency of your system.

System Initialization

System initialization begins when a system is booted. It involves the loading of the operating system and its various components, including the boot process. System initialization is carried out by the *init* program in Linux. The *init* program refers to the configuration file and initiates the processes listed in it. This prepares the system to run the required software. Programs on the system will not run without system initialization.

The *inittab* File

The *inittab* file found in the */etc* directory stores details of various processes related to system initialization. It also stores details of the runlevels in use.

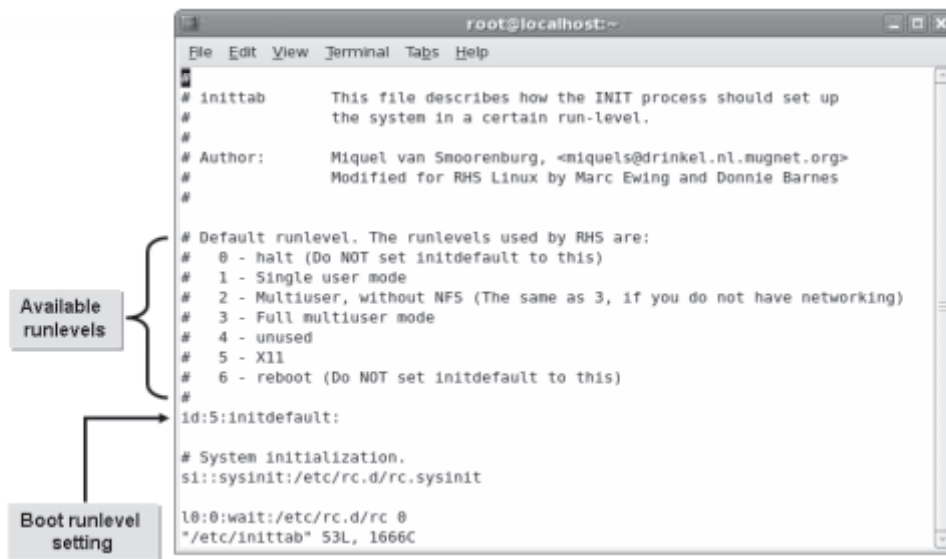


Figure 11-1: The `inittab` file showing runlevel details.

Data Storage Format

The `inittab` file stores data in the `id:runlevels:action:process` format.

The `/etc/init.d` Directory

The `init.d` directory found in the `/etc` directory stores initialization scripts for services. These scripts, called system V scripts, control the initiation of services in a particular runlevel. These runlevels are called system V runlevels. The scripts are invoked from the `/etc/inittab` file when the system initialization begins, using the symbolic links found in the file. System V scripts are highly flexible and can be configured according to the needs of a user. Some of the services listed in the `init.d` directory are `anacron`, `cups`, and `bluetooth`.



Figure 11-2: System and service initialization scripts are found in the `init.d` directory.

Syntax

The syntax for running scripts of the services in the `/etc/init.d` directory is `{service name} {start/stop/status/restart}`.

The chkconfig Command

The `chkconfig` command can be used to control services in each runlevel. It controls services through the symbolic links found in the initialization scripts of services. It can also be used to start or stop services during system startup.

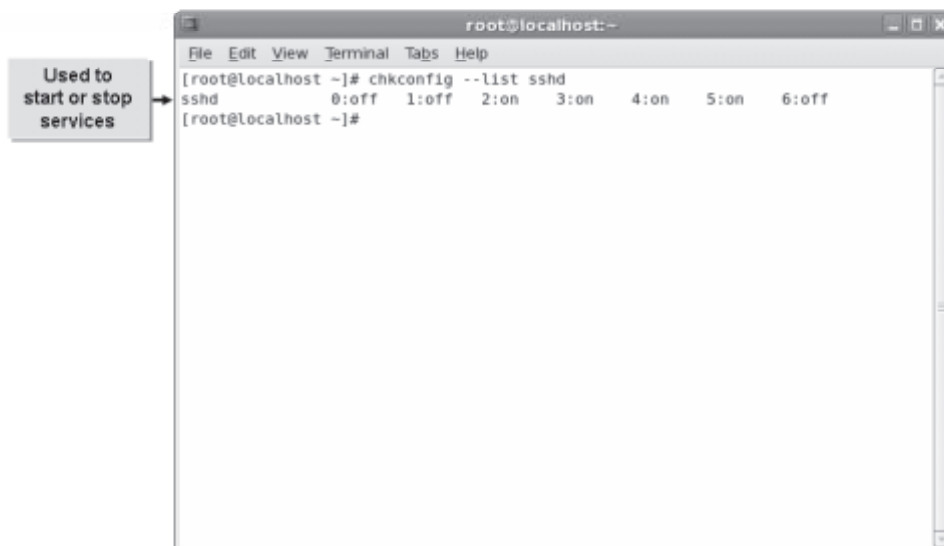


Figure 11-3: *The `chkconfig` command and its options.*

The `chkconfig` command has various options.

Some of the frequently used options are listed in the table.

Option	Enables You To
<code>--level</code>	Specify the runlevel in which the service has to be enabled or disabled.
<code>--add</code>	Add a service to the list of services managed by the <code>chkconfig</code> command.
<code>--del</code>	Delete a service from the list of services managed by the <code>chkconfig</code> command.
<code>--list</code>	List the services managed by the <code>chkconfig</code> command in all runlevels.
<code>on</code>	Start a service at system startup.
<code>off</code>	Stop a service at system startup.
<code>reset</code>	Reset the status of a service.

Syntax

The syntax of the `chkconfig` command is `chkconfig [option] {service name} {on/off/reset}`.

The /etc/sysconfig Directory

The /etc/sysconfig directory contains configuration files for services that should be started at system startup. These files contain settings that describe how these services must be initialized when the system boots. Some of the services listed in the /etc/sysconfig directory include bluetooth, irda, and kdump.



Figure 11-4: The sysconfig directory with various configuration files invoked during system startup.

The system-config-services Command

The system-config-services command enables you to start and stop system services at the current runlevel. It is an X-based graphical utility and should be run on the GUI terminal. The command opens the Service Configuration window, which displays two main tabs: the **Background Services** tab, which is used to control background services and daemons, and the **On Demand Services** tab, which is used to control services managed by the xinetd command.

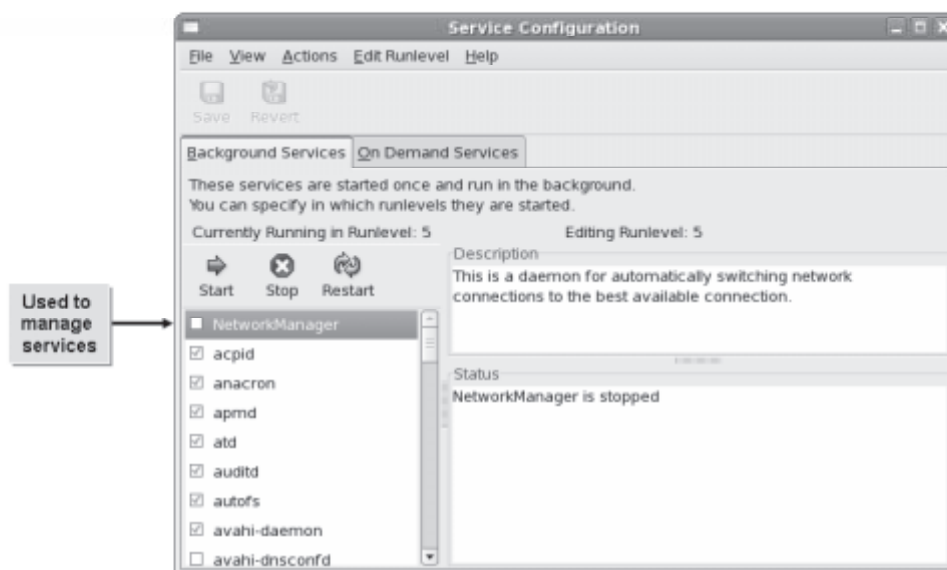


Figure 11-5: *The Service Configuration window.*

The inetd Command

The *inetd* command, also called the Internet “super-server,” is a system service daemon that enables you to start programs needed for accessing different Internet services. When you request for a specific Internet service, *inetd* will start all the related services. It reduces the system load by running one daemon to support several related services without actually running all the daemons at the same time. The *inetd* command uses the */etc/inetd.conf* file to configure services. This command is no longer used in most of the latest versions of Linux distributions and is replaced by the *xinetd* command.

How to Configure System Services

Procedure Reference: Configure Services Using the chkconfig Command

To configure services at different runlevels using the *chkconfig* command:

1. Log in as root.
2. Configure services at different runlevels.
 - To display whether the service name should be stopped or started at each runlevel, enter `chkconfig --list {service name}`.
 - To add a service to *chkconfig* management, enter `chkconfig --add {service name}`.
 - To remove a service from *chkconfig* management, enter `chkconfig --del {service name}`.
 - To stop, start, or reset a service for the mentioned runlevel, enter `chkconfig --level {levels} {service name} {on|off|reset}`.

ACTIVITY 11-1

Enabling a Specific Service

Before You Begin:

- 1. Switch to the GUI.
- 2. The terminal window is displayed.
- 3. To change to the / directory, enter `cd /`.
- 4. To stop the bluetooth service, enter `service bluetooth stop`.
- 5. To turn off the bluetooth service at all runlevels, enter `chkconfig --level 2345 bluetooth off`.
- 6. Close the terminal window.
- 7. Switch to the first terminal in the CLI.
- 8. Log in as root.

Scenario:

As a system administrator, you enabled bluetooth support in one of your systems to enable users to use their bluetooth devices. The users are now complaining that the bluetooth device is not recognized by the system. After troubleshooting, you realize that the problem occurred once the system was restarted. You need to prevent the problem from occurring again.

What You Do	How You Do It
1. Change the status of the bluetooth service at different runlevels.	<ul style="list-style-type: none">a. To check the status of the bluetooth service for different runlevels, enter chkconfig --list bluetoothb. Observe that the bluetooth service is disabled for all runlevels.c. To enable the bluetooth service to run in runlevels 2 to 5, enter chkconfig --level 2345 bluetooth ond. To check whether the status of the service is updated, enter chkconfig --list bluetoothe. Observe that the bluetooth service is now enabled for runlevels 2 to 5.

LESSON 11

2. Start the bluetooth service.

a. To check the current status of the `bluetooth` service, enter **`service bluetooth status`**

b. Observe that the output shows that both `hcid` and `sdpd` are stopped.



The Host Control Interface Daemon (`hcid`) manages all the Bluetooth devices connected to the system.



The Bluetooth Service Discovery Protocol Daemon (`sdpd`) in Linux keeps track of all the bluetooth services registered on the system and responds to inquiries from remote Bluetooth devices.

c. To start the bluetooth service, enter **`service bluetooth start`**

d. Observe that the "OK" status is displayed next to "Starting Bluetooth services," which indicates that the bluetooth service is started successfully.

e. To check the status of the bluetooth service, enter **`service bluetooth status`**

f. Observe that the messages "`hcid (pid {process id}) is running`" and "`sdpd (pid {process id}) is running`" are displayed, which indicate that the `bluetooth` service has started.

g. Clear the terminal screen.

TOPIC B

Monitor System Logs

In the last topic, you configured system services to improve your system's efficiency. To ensure that the changes made to the system services are applied correctly, you need to track the status of each change you make. In this topic, you will monitor system logs.

As a system administrator, you will need to check whether all the changes made to a system are applied, to ensure that the system is working fine. When managing system services, it will be practically impossible to manually track each change made to different services. You can track these changes using the system log files.

System Logs

Definition:

System logs are records of system activities that are tracked and maintained by the syslogd utility. The syslogd utility runs as a daemon. System logs are usually started at boot time. System log messages include the date, the process that delivered the message, and the actual message.

Example:

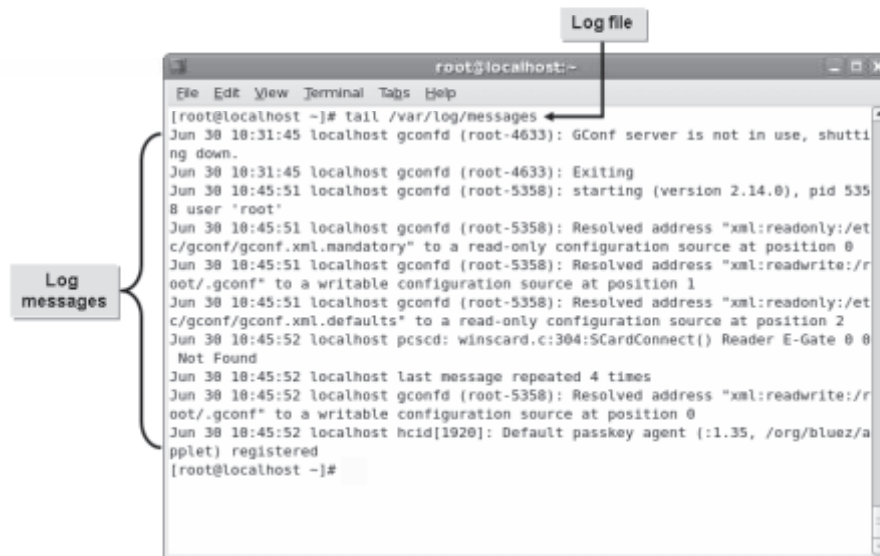


Figure 11-6: System logs and their messages.

Logging Services

A *logging service* is a daemon that is used to track logs or errors that are generated in a system. Log messages are stored in a separate file called the *log file*, which is stored in the `/var/log` directory. The main log file is `/var/log/messages`. In addition to this log file, some services create their own log files.



Figure 11-7: Tracking log files using logging services.

The Central Network Log Server

Definition:

The *central network log server* is a server that is used to implement centralized logging services. This server receives all syslog messages from Linux or Windows servers and from network devices such as routers, switches, firewalls, and workstations, across a network. The server logs data mining and online alerts, performs log analysis, and generates reports.

Example:

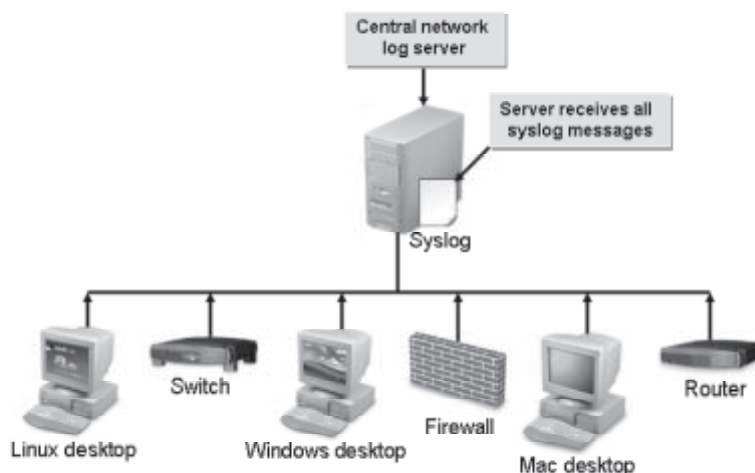


Figure 11-8: The central network log server receiving syslog messages from other servers and network devices.

Automating Log Analysis

During maintenance sessions, instead of manually parsing large log files, you can automate the log analysis by writing Perl or Bash scripts. For example, you can write a Perl script to automatically parse a mail log file and inform you about the rejected email messages. Ensure that you make a `crontab` entry for the script.

Perl

Practical Extraction and Reporting Language (Perl) is a programming language that is used to write scripts. Perl has a powerful feature that is used for manipulating strings; this is why it is extensively used by web servers to process data received from client browsers. In your Perl scripts, you can use `grep` and other textutils to extract specific text from log files.

Automatic Rotation

Automatic rotation is a system of regular rotation of logs to maintain a minimum log file size. The `logrotate` utility is used to perform automatic rotation. When executed, `logrotate` adds a .1 to the end of the file name of the current version of the log files. Previously rotated files are suffixed with .2, .3, and so on. Older logs have larger numbers at the end of their file names. Using automatic rotation, all copies of a file, with dates from when they were created, will be stored. Log files can be rotated on a daily, weekly, or monthly basis. Automatic rotation saves disk space because older log files are pushed out when a size limit is reached.

The syslogd Utility

The `syslogd` utility tracks remote and local system logs. Logs are characterized by their hostname and program field. The settings for `syslogd` are configured using the `/etc/syslog.conf` file.

The syslogd utility

```

root@localhost:~
File Edit View Terminal Tabs Help
[root@localhost ~]# syslogd -d
Allocated parts table for 1024 file descriptors.
Starting.
Called init.
Called allocate_log, nlogs = -1.
cflne(*.info;mail.none;authpriv.none;cron.none      /var/log/messages)
symbolic name: info ==> 6
symbolic name: none ==> 16
symbolic name: mail ==> 16
symbolic name: none ==> 16
symbolic name: authpriv ==> 80
symbolic name: none ==> 16
symbolic name: cron ==> 72
leading char in action: /
filename: /var/log/messages
Called allocate_log, nlogs = 0.
cflne(authpriv.*      /var/log/secure)
symbolic name: * ==> 255
symbolic name: authpriv ==> 80
leading char in action: /
filename: /var/log/secure
Called allocate_log, nlogs = 1.
cflne(mail.*      -/var/log/maillo
g)
  
```

Figure 11-9: Turning on the debug mode in the `syslogd` utility.

The `syslogd` utility provides a number of options to manage specific functions.

Some of the frequently used options are listed in the table.

Option	Used To
<code>-d</code>	Turn on debug mode.
<code>-f {file name}</code>	Specify a new configuration file instead of <code>/etc/syslog.conf</code> .
<code>-m {interval}</code>	Specify a time interval between two mark timestamp lines in the log.
<code>-r</code>	Enable the <code>syslogd</code> utility to receive messages from a network.

Syntax

The syntax of the `syslogd` utility is `syslogd [options]`.

logger

The logger is the command interface to the system log module. The logger has options that allow you to customize the content that needs to be logged.

The klogd Utility

The *kernel logging daemon (klogd)* tracks kernel messages by prioritizing them. It listens to the source for kernel messaging and intercepts the messages. klogd runs as a client of syslogd, where the kernel messages are sent through the syslogd daemon. klogd also acts as a standalone program.

The klogd command provides a number of options to manage specific functions. Some of the frequently used options are listed in the table.

Option	Enables You To
-c {n}	Set the default log level to n for messages, where n ranges from 0 to 7. <ul style="list-style-type: none">• 0–Emergency• 1–Alert• 2–Critical• 3–Error• 4–Warning• 5–Notice• 6–Information• 7–Debug
-p	Load the kernel module symbol information.
-k {file name}	Use the specified file as the source to store the kernel module symbol information.
-o	Read and log all kernel messages in the buffer in a single read.
-d	Switch to debugging mode.
-f {file name}	Log messages to the file that is specified.
-s	Use the system call interface for buffering the kernel messages.

Syntax

The syntax of the klogd command is klogd [options].

The /etc/syslog.conf File

The */etc/syslog.conf* file controls the location where the syslogd information is recorded. This file consists of two columns. The first column lists the facilities and severities of the messages. The second column lists the files the messages should be logged to. By default, most messages are stored in the */var/log/messages* file.

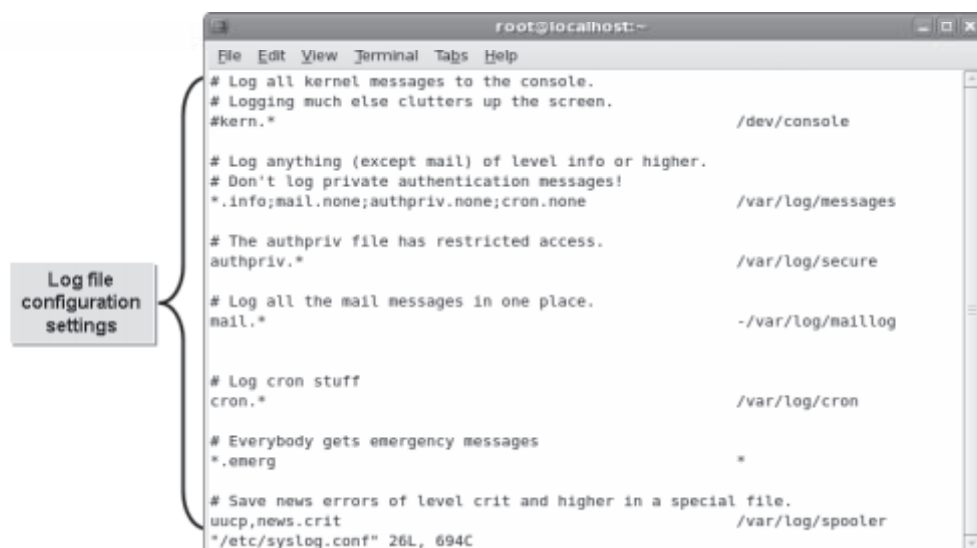


Figure 11-10: The `syslog.conf` file with the logging configuration settings.

Some applications maintain their own log files and directories independent of the `syslog.conf` file. Each service has its own log storage file. Some of the frequently used log files are listed in the table.

Log File	Description
<code>/var/log/syslog</code>	Stores the system log file, which contains information about the system.
<code>/var/log/maillog</code>	Stores mail messages.
<code>/var/log/samba</code>	Stores Samba messages.
<code>/var/log/mrtg</code>	Stores Multi Router Traffic Grapher (MRTG) messages.
<code>/var/log/httpd</code>	Stores Apache web server messages.

MRTG

MRTG is free software, licensed under GPL, that is used to monitor and measure the traffic load on network links. The traffic load on a network is represented in graphical form.

Log File Analysis

The process of examining messages generated by logging daemons in log files is referred to as *log file analysis*. Log messages are created in a format that is specific to an application or a vendor and are arranged in chronological order. During analysis, the format of log messages from different logging sources, such as operating systems, networks, and databases, is compared with a preset format. Also, log messages are categorized for each user with respect to the application, system, or system configuration accessed, to ensure user authentication.

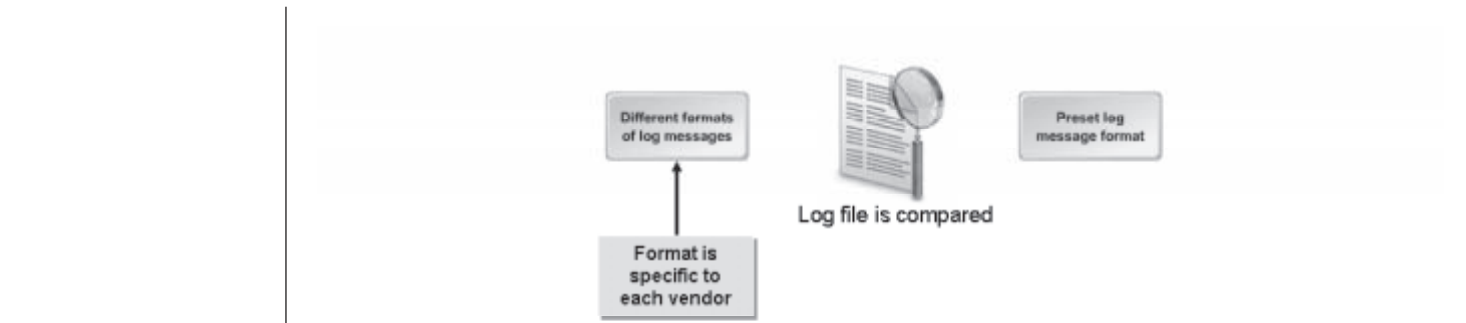


Figure 11-11: Various steps involved in log file analysis.

The lastlog Command

The *lastlog* command utilizes data from the `/var/log/lastlog` file to display the latest login details of all users. In addition to the login name, date, and time, it displays the terminal from where a user last logged in. The *lastlog* command is used by administrators to view user accounts that have never been used.

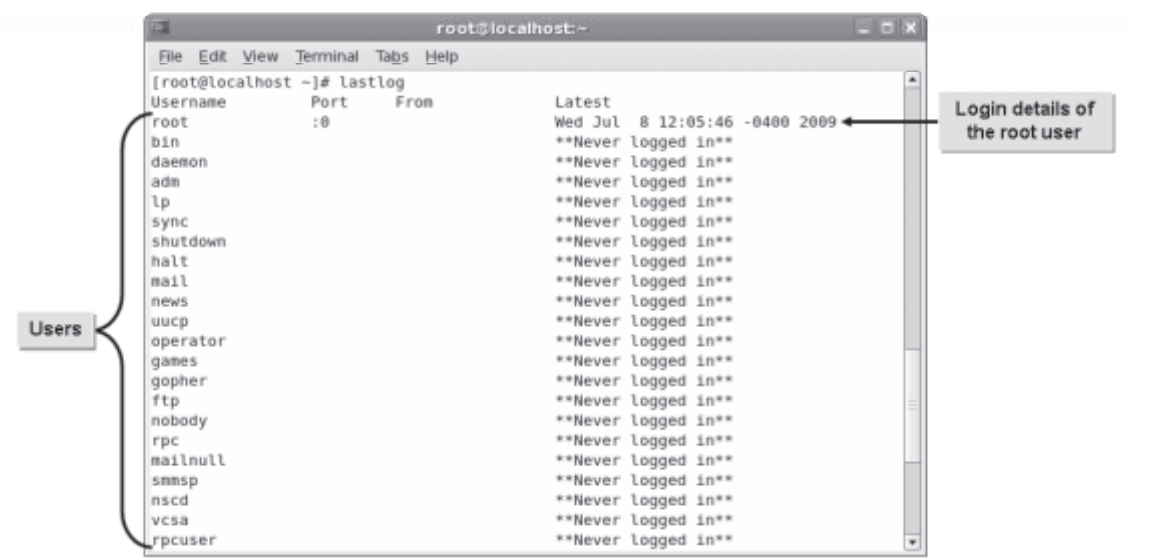


Figure 11-12: The output of the lastlog command.

The grep Command

The *grep* command searches a file or list of files for a string and prints the lines that match the search string. The *grep* command has various options that allow you to specify search criteria.

The following table lists the options of the *grep* command.

Option	Used To
-h	Print matching lines without file names.
-w	Restrict the search to whole words only.

Option	Used To
-c	Display a count of the number of matching lines and not the lines themselves.
-i	Ignore case while searching.
-l	List the file names that contain matching lines.
-n	Precede each line with the line number where it was found.
-s	Suppress the display of any error message.
-e	Specify one or more patterns for searching.

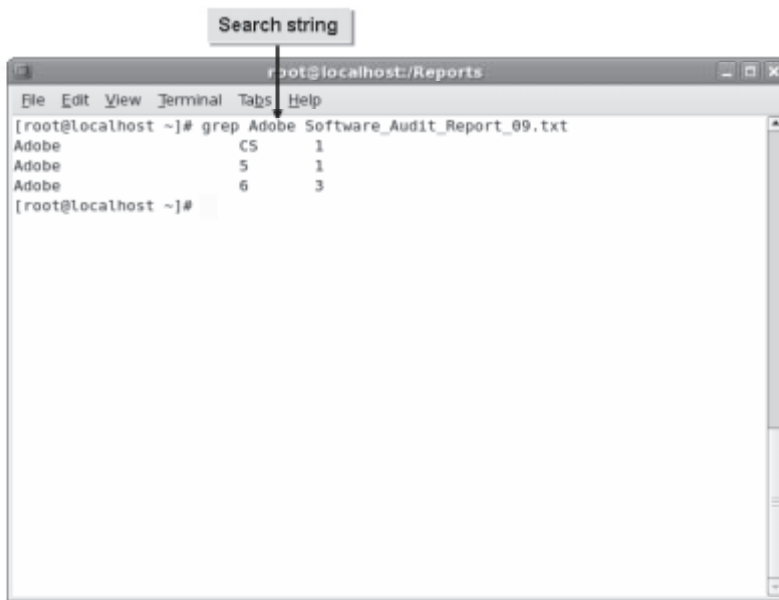


Figure 11-13: The *grep* command is used to search for a string in a file.

Syntax

The syntax of the *grep* command is *grep [options] {keyword} {file name}*.

fgrep and egrep Commands

The *fgrep* command searches for multiple text patterns; however, this command's search is not based on regular expressions.

The *egrep* command searches for multiple text patterns, which may include a larger set of regular expression elements than *grep*.

The tail Command

The *tail* command is used to retrieve data from a file. By default, it displays the last 10 lines of the file. The *tail* command has various options.

Some of the frequently used options are listed in the table.

Option	Enables You To
<code>--retry</code>	Force the <code>tail</code> command to open a file that cannot be opened.
<code>-c {total no. of bytes}</code>	Print the specified number of bytes from the end of a file.
<code>-f</code>	Update the output of the <code>tail</code> command if any change is made to a file.

```

root@localhost:~/Policies
File Edit View Terminal Tabs Help
[root@localhost ~]# tail Training_Policy.txt
Communication & Presentation
Team Working Program
Performance Feedback
Time Management
Stress Management
Positive Thinking

*(The list is dynamic new programs shall be added based on competency)

Programs may also include guest lectures.
[root@localhost ~]#
  
```

Figure 11-14: The output of the `tail` command.

Syntax

The syntax of the `tail` command is `tail [options] {file name}`.

The `awk` Command

The `awk` command is a command that performs pattern matching. GNU's version of `awk` is called `gawk`. The `awk` keyword is followed by the pattern, the action to be performed, and the file name. The action to be performed is given within curly braces. The pattern and the action to be performed should be specified within single quotes. If the pattern is not specified, the action is performed on all input data; however, if the action is not specified, the entire line is printed. The `awk` command can be executed from the command line or from within an `awk` script file.

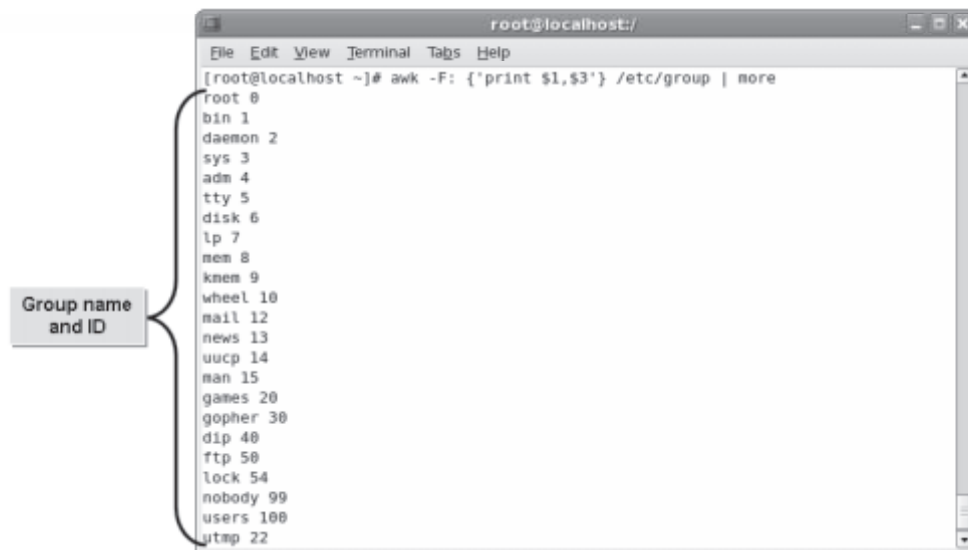


Figure 11-15: Using the `awk` command to display only the group name and ID from the `/etc/group` file.

Syntax

The syntax of the `awk` command is `awk [options] {file name}`.

Patterns

In `awk` scripts, you can provide patterns along with blocks of code. If a pattern matches any line in the input file, the code blocks in the script will be executed. The following table lists the types of patterns used.

Pattern	Description
<code>/regular_expression/</code>	Retrieves all the records beginning with “a,” “b,” or “c.” Example: <code>/[abc]/</code>
<code>relational_expression</code>	Retrieves all the records whose first field contains the value “abc.” Example: <code>\$1 == “abc”</code>
<code>pattern_1 && pattern_2</code>	Retrieves all the records whose first field contains the value “abc” and the second field contains the value “01.” Example: <code>(\$1 == “abc”) && (\$2 == “01”)</code>
<code>pattern_1 pattern_2</code>	Retrieves records that satisfy the condition that the first field contains the value “abc” or the second field contains the value “01,” or both. Example: <code>(\$1 == “abc”) (\$2 == “01”)</code>

Pattern	Description
<code>pattern_1 ? pattern_2 : pattern_3</code>	If the first field in a record contains the value “10,” the fifth field is tested for its value. If the fifth record contains the value “20,” then the record is printed. If the first field of a record does not contain the value “10,” then the ninth field of the record is evaluated. If the ninth record contains the value “30,” then the record is printed. Example: <code>\$1 == “10” ? \$5 == “20” : \$9 == “30”</code>
<code>pattern_1, pattern_2</code>	Prints a range of records, starting from the record whose first field contains the value “01.” The records will be printed until the <code>awk</code> command finds a record whose first field contains the value “02.” Example: <code>\$1 == “01”, \$1 == “02”</code>

The sed Command

The `sed` command is a command line program that can be used to modify log files or text files according to command line parameters. The `sed` command can be used for global search and replace actions. The `sed` command has various options.

Some of the common `sed` command options and their uses are given in the following table.

Option	Used To
<code>d</code>	Delete the lines that match a specific pattern or line number.
<code>-n, p</code>	Print only the lines that contain the pattern.
<code>s</code>	Substitute the first occurrence of the string in the file.
<code>s, g</code>	Substitute globally the original string with the replacement string for each occurrence in the file.

Syntax

The general syntax of the `sed` command is `sed '{address/pattern/action}' {file name}`. If there is an address, it follows the command name. The pattern formed by the user comes next, followed by the action to be performed when a match is found. The last argument is the name of the input file. The address, pattern, and action parameters are enclosed within single quotation marks.

How to Monitor System Logs

Procedure Reference: Configure System Logs

To configure system logs:

1. Log in as root.
2. To open the configuration file, enter `gedit /etc/syslog.conf`.
3. To set the type and level of severity to be logged in the specified file, type `{facility}.{level of severity} / {location of the file that stores the log messages}`.
4. Save and close the file.
5. To restart the system log service and apply the changes, enter `service syslog restart`.

Procedure Reference: Configure syslogd to Act as a Central Network Log Server

To configure syslogd to act as a central network log server:

1. Log in as root in the CLI.
2. To open the syslog file, enter `gedit /etc/sysconfig/syslog`.
3. To add the **-r** option to the **SYSLOGD_OPTIONS** parameter, type `SYSLOGD_OPTIONS="-r -m 0."`.
4. Save and close the file.
5. To restart the syslog service, enter `service syslog restart`.

Procedure Reference: Configure syslogd to Send Log Output to a Central Log Server

To configure syslogd to send the log output to a central log server:

1. Log in as root.
2. To open the system log configuration file, enter `gedit /etc/syslog.conf`.
3. To send the log output to a remote log server, type `{facility} {level of severity} @{IP or FQDN of the log server}`.
4. Save and close the file.
5. To restart the system log service and apply the changes, enter `service syslog restart`.

Procedure Reference: Search and Replace Strings

To search and replace strings:

1. Log in as a user in the CLI.
2. Search and replace strings.
 - To replace the old string with the replacement string even if multiple occurrences of the old string are found in a single line, enter `sed 's/{old string}/{replacement string}/g' {file name}`.

- To replace only the first occurrence of the old string with the replacement string even if multiple occurrences of the old string are found in a single line, enter `sed 's/{old string}/{replacement string}' {file name}`.

Procedure Reference: Extract Information Manually from Log Files

To extract information manually from log files:

1. To view the current list of system log files, enter `ls /var/log`.
2. Use suitable commands to extract information from log files.
 - To print the output of specific columns from the selected file, enter `awk '{print ${column name} ${column name}}' {file name}`.
 - To manually scan the log files and extract values that match the specific activity, enter `grep -r "{d} {file name}"`.

ACTIVITY 11-2

Configuring System Log Settings

Before You Begin:

1. You have logged in as root in the CLI.
2. Switch to the GUI.

Scenario:

As the system administrator, you regularly perform routine maintenance checks on network systems. You find that the logs show a couple of errors because they were not entered properly. You want only the warnings and alerts to be shown in the logs. So, you decide to configure the settings for `syslog`.

What You Do	How You Do It
1. Open the <code>/etc/syslog.conf</code> file.	<ol style="list-style-type: none">a. To open the terminal window, choose Applications→Accessories→Terminal.b. To open the <code>syslog.conf</code> file in the <code>gedit</code> program, enter gedit /etc/syslog.confc. To move to the last line of the file, press Ctrl+End.

2. Configure the `syslog` settings.
 - a. To set the severity of the error to be logged for mail messages, type **mail 4 /var/log/test.log**
 - b. To save the file, choose **File→Save**.
 - c. To close the file and exit the **gedit** editor, choose **File→Quit**.
 - d. To restart the `syslog` service, in the terminal window, enter **service syslog restart**
 - e. To clear the terminal window, enter **clear**

ACTIVITY 11-3

Configuring Syslogd

Before You Begin:

1. You have logged in as root in the GUI.
2. The terminal window is displayed.

Scenario:

As a system administrator, you want your system to act as the central server to store all system logs to easily track activities. To implement this, you connect additional users to your system. However, you want the messages to be automatically sent to your system and do not want to monitor each system individually. So, you decide to configure the system logs to accomplish your task.

What You Do	How You Do It
1. Configure <code>syslogd</code> to act as a central network log server.	<ol style="list-style-type: none"> a. To open the <code>syslog</code> file in the <code>gedit</code> program, enter gedit /etc/sysconfig/syslog b. To specify the line number to navigate to, choose Search→Go to Line. c. To navigate to the sixth line containing <code>SYSLOGD_OPTIONS="-m 0,"</code> in the text box, enter 6

LESSON 11

2. Modify the settings in the `/etc/sysconfig/syslog` file.
 - a. Position the cursor between `"` and `-m` in `SYSLOGD_OPTIONS="-m 0."`
 - b. Add the `-r` option to the `SYSLOGD_OPTIONS` parameter to set it as `SYSLOGD_OPTIONS="-r -m 0."`
 - c. To save the file, choose **File→Save**.
 - d. To close the file and exit the **gedit** editor, choose **File→Quit**.
 3. Restart the syslog service.
 - a. To restart the syslog service, enter **`service syslog restart`**
 - b. To clear the terminal window, enter **`clear`**
-
-

ACTIVITY 11-4

Analyzing Log Files

Before You Begin:

1. You have logged in as root in the GUI.
2. The terminal window is displayed.
3. Switch to the first terminal in the CLI.

Scenario:

Your manager asked you to analyze log files and document the results. To do this, you need to:

- Monitor the usage of the root login to prevent unauthorized usage.
- Prepare a list of users with their login name, GID, and home directory.
- Generate a report with the group name and GID.

What You Do	How You Do It
1. Locate the instances of root login usage.	<ol style="list-style-type: none">To change to the log directory, enter <code>cd /var/log</code>To display the results of the root login, enter <code>grep "ROOT LOGIN" secure</code>Observe the login details displayed in the results. To clear the terminal screen, enter <code>clear</code>
2. Generate a list of users with their login name and other details.	<ol style="list-style-type: none">To change to the etc directory, enter <code>cd /etc</code>To list the login name, GID, and home directory for all users, enter <code>awk -F: {'print \$1,\$3,\$6'} passwd</code>Observe the details displayed for the user accounts. To clear the terminal screen, enter <code>clear</code>
3. Generate a list of groups with GID.	<ol style="list-style-type: none">To list the group name and GID for all groups, enter <code>awk -F: {'print \$1,\$3'} group</code>Observe the details displayed for the group accounts.To clear the terminal screen, enter <code>clear</code>

TOPIC C

Configure SELinux

Previously, you monitored system log files to ensure that the changes made to the services are applied correctly. Information on a system needs to be protected from misuse or damage by using appropriate security measures such as SELinux. In this topic, you will configure SELinux.

Even when a server is configured and running correctly, it is possible that security attacks may occur, which could be aimed at both organizations and individuals. Imagine that your company's servers are damaged and all your critical data are erased. You can prevent this by setting up the required security checks using SELinux.

Types of Access Controls

Access control is a method of restricting access to system resources. Only authorized programs will be allowed to access system resources. In Linux, there are two types of access controls.

Access Control Method	Description
Discretionary Access Control (DAC)	<p>In DAC, the system checks the resources over which a user has access rights. The rights of the user are identified using the authentication information such as user identity and password.</p> <p>Under DAC, there are two types of permissions: the administrator permissions and the non-administrator permissions. For application programs to run, administrator access has to be provided. Administrator access provides full discretion over the filesystem and exposes it to security threats.</p> <p>For example, a malicious program or process started by a user having administrator access can damage data in a filesystem.</p> <p>DAC is the standard security strategy in Linux.</p>

Access Control Method	Description
Mandatory Access Control (MAC)	<p>In MAC, the system checks the resources over which a user does not have access rights. MAC is applied through SELinux. The rights of the user are identified using authentication such as the SELinux user identity, role, and type of access. MAC is the opposite of DAC, where permissions have to be defined for all processes (known as subjects) as to how they access resources (known as objects) such as files, directories, devices, memory resources, and other processes. An action is an operation, such as append, write, read, create, execute, and rename, that a subject can perform on an object. This is implemented using security policies that control the interaction between the processes and the objects.</p> <p>For example, when a subject tries to access an object, the security policy is checked to verify whether the subject is authorized to access the object before granting the access.</p>

Security-Enhanced Linux

Security-Enhanced Linux (SELinux) is the default security enhancement feature provided with Red Hat Enterprise Linux, and is available on other distributions. It was developed by the U.S. National Security Agency while implementing various security policies on Linux operating systems. It provides additional filesystem and network security so that unauthorized processes cannot access or tamper with data, bypass security mechanisms, violate security policies, or execute untrustworthy programs. It enforces MACs on processes and resources and allows information to be classified and protected based on its confidentiality and integrity requirements. This confines the damage caused to information by malicious applications.

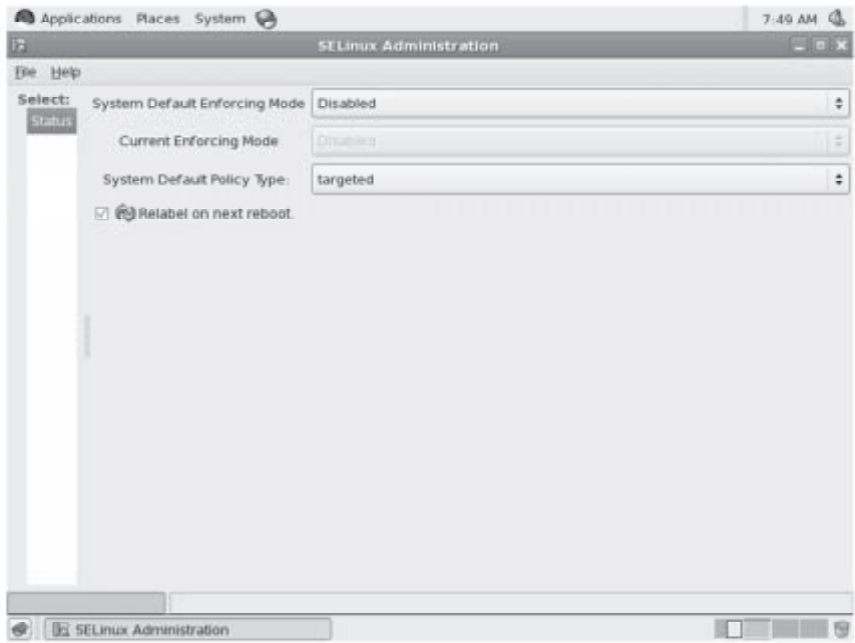


Figure 11-16: The SELinux feature of Red Hat Enterprise Linux 5.

 The SELinux feature comes as part of Red Hat Enterprise Linux (RHEL) 4 and the later versions.

SELinux Modes

SELinux has three different modes.

Mode	Description
Disabled	In this mode, SELinux is turned off. So, MAC will not be implemented and the default DAC method will be prevalent.
Enforcing	In this mode, all the security policies are enforced. Therefore, processes cannot violate the security policies.
Permissive	In this mode, SELinux is enabled, but the security policies are not enforced. So, processes can bypass the security policies. However, when a security violation occurs, it is logged and a warning message is sent to the user.

Security Policies

A security policy defines access parameters for every process and resource on the system. Configuration files and policy source files located in the /etc/selinux directory can be configured by the root user.

Security Policy Type	Description
Targeted	According to the targeted policy, except the targeted subjects and objects, all other subjects and objects will run in an unconfined environment. The untargeted subjects and objects will operate on the DAC method and the targeted ones will operate on the MAC method. A targeted policy is enabled by default.
Strict	A strict policy is the opposite of a targeted policy, where every subject and object of the system is enforced to operate on the MAC method. However, a strict policy is not available in SELinux of the RHEL 5 version.

How to Configure SELinux

Procedure Reference: Control the SELinux State on the System

To control the SELinux state on the system:

1. Log in as root in the GUI.
2. Control the SELinux state on the system.
 - Control the SELinux state using the `/etc/sysconfig/selinux` file.
 - a. To open the `selinux` file, enter `vi /etc/sysconfig/selinux`.
 - b. Switch to insert mode.
 - c. To change the `SELINUX` variable to control the mode of the SELinux policy, set `SELINUX={enforcing | permissive | disabled}`.
 - d. To change the `SELINUXTYPE` variable to control the type of the SELinux policy, set `SELINUXTYPE={targeted | strict}`.
 - e. Save and close the file.
 - Switch between enforcing mode and permissive mode.
 - a. To switch between enforcing mode and permissive mode, enter `setenforce {1 | 0}`, respectively.
 - b. To view the mode, enter `getenforce`.
 - Control the SELinux state using GUI tools.
 - a. Open the SELinux Administration window.
 - To open the **SELinux Administration** utility, enter `system-config-selinux`.
 - In **GNOME Panel**, choose **System**→**Administration**→**SELinux Management**.
 - b. Manage the SELinux settings.
 - To manage the mode and the policy type that are in the right pane, in the left pane, select **Status**.

- To manage individual policies related to services that are in the right pane, in the left pane, select **Boolean**.
- If necessary, change other settings.
- To close the SELinux Administration window, on the menu bar, choose **File**→**Quit**.

Procedure Reference: View the Security Context for Files and Processes

To view the security context for files and processes:

1. Log in as root in the CLI.
2. View the security context for files and processes.
 - To view the security context of the specified file or directory, enter `ls -Z[options] {file or directory name}`.
 - To view the security context of the specified process, enter `ps -Z[options] {process name}`.

Security Context

Security context is the collection of all security settings pertaining to processes, files, and directories. Security context consists of three elements: user, role, and type. Based on the security context attributes, SELinux decides how subjects access objects on the system.

Procedure Reference: Change the Security Context for Files

To change the security context for files:

1. Log in as root in the CLI.
2. Change the security context for files.
 - To set the specified security context to the specified file or directory, enter `chcon -[options] {security context} {file or directory name}`.
 - To restore the default security context to the specified file or directory, enter `restorecon {file or directory name}`.

ACTIVITY 11-5

Configuring SELinux

Before You Begin:

On srvA, you have logged in as root in the CLI.

Scenario:

Your system contains confidential information that needs to be protected from any unauthorized access. You need to enable access control to prevent processes from reading or tampering data and programs, bypassing application security mechanisms, executing unauthorized programs, or interfering with other processes in violation of the system security policy.

What You Do	How You Do It
1. Configure SELinux mode.	<ul style="list-style-type: none">a. To configure the SELinux settings, enter vi /etc/sysconfig/selinuxb. To go to the SELinux mode configuration line, enter /SELINUX=disabledc. To switch to insert mode, press I.d. To configure access control, set SELINUX=permissive.
2. Check whether the SELinux policy settings are set.	<ul style="list-style-type: none">a. Verify that the security policy is set to SELINUXTYPE=targeted.b. To switch to command mode, press Esc.c. Save and close the file.d. To apply the settings, enter reboot

Lesson 11 Follow-up

In this lesson, you configured system services, monitored system logs, and configured SELinux. This will enable you to utilize your Linux system at its optimum level.

1. **How will you use system logs to troubleshoot system problems?**
2. **Why is access control required?**

LESSON 12

Configuring Network Services

Lesson Time

3 hour(s), 30 minutes

In this lesson, you will configure Linux services to provide users with network connectivity.

You will:

- Connect to a network.
- Configure routes.
- Configure client network services.
- Manage remote network systems.

Introduction

In the last lesson, you configured basic system services on your computer. Sometimes, you may need to establish a connection with other computers to communicate with them. In this lesson, you will configure network services.

A network enables computers to communicate with each other and share data, software, and hardware resources. Network services allow system administrators to disseminate information, administer systems remotely, enable communication through mail or chat systems, facilitate technology sharing, manage software licenses, and control unauthorized access.

This lesson covers all or part of the following CompTIA Linux+ Powered by LPI certification objectives:

- Topic A:
 - Objective 109.1, Objective 109.2, Objective 109.3, Objective 110.2
- Topic B:
 - Objective 109.1, Objective 109.2, Objective 109.3, Objective 110.1
- Topic C:
 - Objective 109.1, Objective 109.2, Objective 109.3, Objective 109.4
- Topic D:
 - Objective 110.3

TOPIC A

Connect to a Network

In the last lesson, you worked with data and other utilities solely on your computer. Sometimes, you may need to share data and devices with other computers on a network. In this topic, you will connect to a network.

As a network administrator, you may need to manage and troubleshoot servers, network services, and workstations. To manage a network, you should understand the basic concepts of a network and its components. By connecting to a network, you will be able to implement network services required to efficiently manage a network with numerous systems.

Networks

Definition:

A *network* is a group of computers connected together to communicate with each other and share resources. Each device on the network is referred to as a node. The components of a network are servers; clients; communication cables; resources, such as files or printers; network adapters; and network protocols.

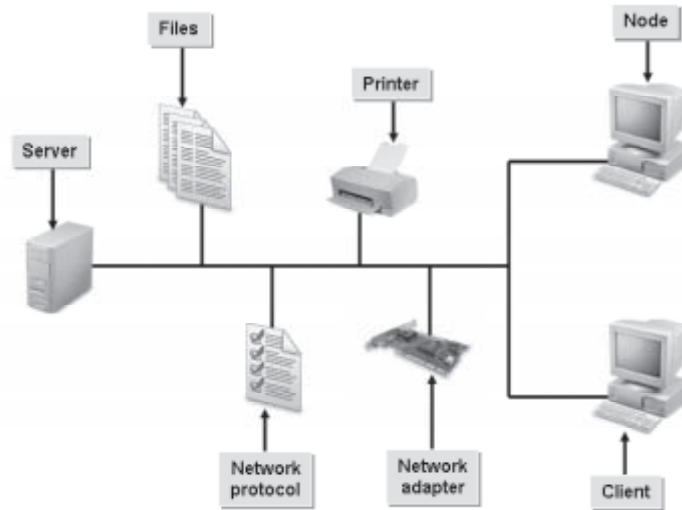
Example:

Figure 12-1: An example of a network.

Types of Networks

Networks can be broadly classified into two types based on their size.

Network Type	Description
<i>Local Area Network (LAN)</i>	A network that connects computers in a small geographical area such as a floor or a building. Computers on a LAN are connected through Ethernet at speeds of 10 Mbps, 100 Mbps, or 1,000 Mbps. Compared to other types of networks, such as MAN and WAN, a LAN is a high-speed data network.
<i>Wide Area Network (WAN)</i>	A network that connects computers in a wide geographical area. Computers on a WAN are connected through bridges, routers, hubs, and repeaters. This network can extend across a country or around the world. A WAN may connect LANs and MANs.

Metropolitan Area Networks

A *Metropolitan Area Network (MAN)* is a network that connects computers in a broad geographical area such as a city and its suburbs. Computers on a MAN are connected through switches, access servers, and ISDN terminal adapters. This network is a medium-speed data network and can connect two or more LANs.

Network Protocols

Definition:
A *network protocol* is a set of rules that enable communication and data transfer among network devices. The rules specify how data should be shared among systems. Network protocols include conventions that specify message acknowledgment or data compression.

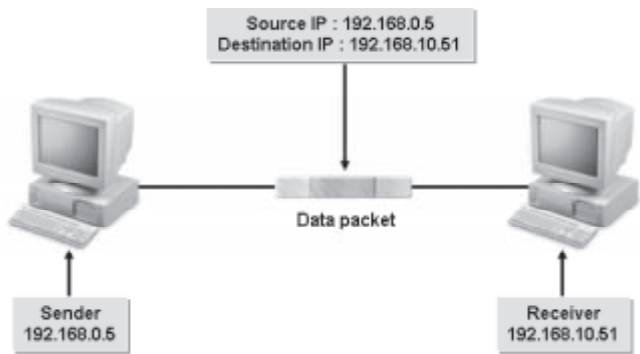


Figure 12-2: Data transmitted between two computers on a network.

Example: Data Transfer
A network protocol contains rules that establish the method by which data is transmitted virtually on all networks today. It transmits data to the destination and acknowledges the source to ensure that the data is delivered.

Types of Network Protocols

A network protocol is chosen based on the network setup and network requirements. The protocols range from a high level to a low level, based on the network capacity.

Network Protocol	Used To
<i>Transmission Control Protocol/Internet Protocol (TCP/IP)</i>	Transfer packets of data from one system to another on a network. TCP binds with IP and acts as a core layer for the Internet. TCP/IP guarantees that the packets are delivered in the same order in which they are sent.
<i>HyperText Transfer Protocol (HTTP)</i>	Transfer hypertext files across the World Wide Web. HTTP allows web browsers and web servers to communicate with each other to request a file and transfer contents. There are many versions of HTTP.
<i>File Transfer Protocol (FTP)</i>	Send and receive files over the Internet. FTP is based on the client/server architecture. A user with an FTP client has to log on to a remote system, navigate to the filesystem, and upload and download files from that system.

Network Protocol	Used To
<i>Internet Control Message Protocol (ICMP)</i>	Handle error and control messages. It does not transfer any application data, but transfers information about the status of the network. The <i>ping</i> utility uses ICMP for probing messages. It is useful in Internet protocol network management and administration.
<i>User Datagram Protocol (UDP)</i>	Transmit data in the form of small packets that are sent independently. This protocol cannot determine whether the data reached its destination or not. It is a transport protocol that is part of the TCP/IP suite of protocols.

IP Addresses

An *IP address* is a unique address that identifies a host on the Internet. It is a 32-bit binary number that is displayed as four decimal numbers, called octets, separated by periods. For example, 155.40.104.49 is an IP address.

The first two octets of the address identify the network on which a host resides and the next two octets identify the host.

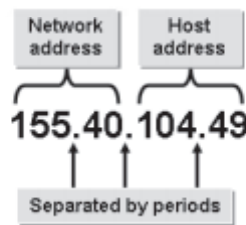


Figure 12-3: An IP address that identifies the network on which a host resides.

IP Versions

IP Version 4 (IPv4) and *IP Version 6 (IPv6)* are the two versions of the Internet protocol that are currently in use. With the number of hosts on the Internet growing at a fast pace, the earlier version, IPv4, which adopts a 32-bit addressing format, has limited unique IP addresses for public Internet access, in addition to reserved and consumed addresses. There is a chance of running out of IP addresses and routing can become complicated. This can restrict future Internet access.

So, a new version of IP, called *IP Next Generation (IPng)* or IPv6, is implemented on the Internet. The proposed Internet standard can increase the available pool of IP addresses by implementing a 128-bit binary address space. IPv6 also includes new efficiency features such as simplified address headers, hierarchical addressing, support for time-sensitive network traffic, and a new structure for unicast addressing.

IPv6 and IPv4 Compatibility

IPv6 is not compatible with IPv4; so at present, it is deployed on a limited number of test and production networks. Full adoption of the IPv6 standard will require a general conversion of IP routers to support interoperability.

Comparing IPv4 and IPv6

IPv4 and IPv6 differ drastically in several key areas. The major differences are shown in the following table.

IPv4	IPv6
Uses 32 bit addresses.	Uses 128 bit addresses.
ARP uses broadcast ARP request to resolve IP to MAC/Hardware address.	Multicast Neighbor Solicitation messages resolve IP addresses to MAC addresses.
Addresses are distributed by DHCP or are manually configured.	Addresses are distributed by Neighbor Discovery Protocol, DHCPv6, or manually.
Headers include a Checksum.	Headers do not include a Checksum.
576 Byte packet size.	1280 Byte packet size.
Broadcast addresses send to all network nodes.	Does not use Broadcast.
Routers and hosts may fragment packets.	Routers do not perform fragmentation.
Host names are mapped to IP Addresses using A records.	Host names are mapped to IP Addresses using AAAA (quad-A) records.

IP Classes

An *IP class* is a block of IP addresses that can be assigned to businesses or governments, based on the size and need. Each IP address belongs to an IP class. There are five IP classes: Class A, Class B, Class C, Class D, and Class E. The octets in the IP addresses are used to create the IP classes. IP classes are assigned by the Internetwork Information Center, or InterNIC.

Each IP class has different criteria for its usage as listed below.

- Class A—Used for very large networks.
- Class B—Used for medium-size networks.
- Class C—Used for small to medium-size businesses.
- Class D—Used for multicasts (Eg: Cisco router sending an update to all other Cisco routers.)
- Class E—Used for experimental purposes.

Private Networks

Three IP network address blocks are reserved for private networks, or intranets.

- 10.0.0.0 to 10.255.255.255
- 172.16.0.0 to 172.31.255.255
- 192.168.0.0 to 192.168.255.255

These addresses can be used for setting up internal IP networks, such as an organization's LAN. Routers on the Internet will not forward packets coming from these addresses. These addresses are meaningful only for the network to which they belong. Within these range of addresses, two or more organizations can have the same IP address assigned to a machine. In addition to these three IP network addresses, 127.0.0.1 is reserved as a loopback address.

Subnet Masks

Definition:

A *subnet mask* is a 32-bit number that is assigned to each system to divide the 32-bit binary IP address into network and node portions. This makes TCP/IP routable. A subnet mask uses a binary operation to remove the node ID from the IP address, leaving just the network portion. The network portion of an IP address can also be referred to as a netmask. Subnet masks use the value of eight 1s in binary, or 255 in decimal, to mask an entire octet of the IP address. A subnet mask acts as a filter that tells the server whether an IP address is on a local network or on a remote network. Subnet masks help routers identify whether a data packet needs to be retained on the local network or sent to another network.

Example:

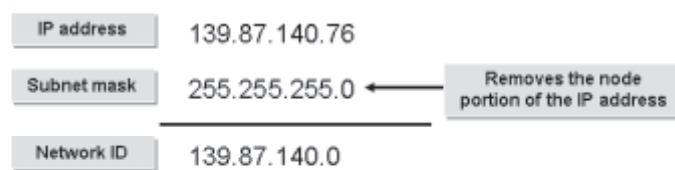


Figure 12-4: *The subnet mask removes the node portion of the IP address.*

Subnet Mask Values

The table lists the subnet mask values.

Subnet Mask	Number of Subnets	Number of Hosts In Class A	Number of Hosts In Class B	Number of Hosts In Class C
128	2	8,388,606	32,766	126
192	4	4,194,302	16,382	62
224	8	2,097,150	8,190	30
240	16	1,048,574	4,094	14
248	32	524,286	2,046	6
252	64	262,142	1,022	2
254	128	131,070	510	0
255	256	65,534	254	0

IP Address Classes

The designers of the TCP/IP suite defined five ranges of addresses, called address classes, for specific network uses and sizes. Changes in the Internet, since the early 90s, have rendered classful addresses obsolete. One of the final remnants of classful addressing is the use of the terms Class A, Class B, and Class C to describe common subnet masks.

Class and Subnet Mask	Description
Class A 255.0.0.0	<p><i>Class A</i> subnet masks provide a small number of network addresses for networks with a large number of nodes per network.</p> <ul style="list-style-type: none"> • Number of nodes per network: 16,777,214 • Network ID portion: First octet • Node ID portion: Last three octets <p>Class A addresses are used only by extremely large networks. Large telephone companies and ISPs leased most Class A network addresses early in the development of the Internet.</p>
Class B 255.255.0.0	<p><i>Class B</i> subnet masks offer a larger number of network addresses, each with fewer nodes per network.</p> <ul style="list-style-type: none"> • Number of nodes per network: 65,534 • Network ID portion: First two octets • Node ID portion: Last two octets <p>Most companies leased Class B addresses to use them on Internet-connected networks. In the beginning, there were plenty of Class B addresses to go around, but now there are a few.</p>
Class C 255.255.255.0	<p><i>Class C</i> subnet masks offer a large number of network addresses for networks with a small number of nodes per network.</p> <ul style="list-style-type: none"> • Number of nodes per network: 254 • Network ID portion: First three octets • Node ID portion: Last octet <p>Because there can be more Class C networks than any other type, they are the only addresses still available.</p>

Classless Addressing

Because the traditional IP address classes have limitations on the number of available addresses in each class, there are now various implementations that utilize classless addressing. In these schemes, there is no strict dividing line between groups of addresses, and the network address or node address division is determined entirely by the number of 1 bits in the subnet mask.

Broadcast Addresses

Definition:

A *broadcast address* is a special IP address that is used to send messages to all hosts with the same network address. On IP networks, the general broadcast address is 255.255.255.255.

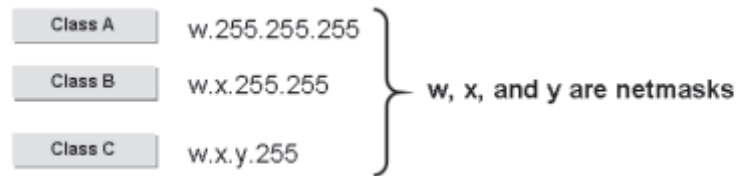
Example:

Figure 12-5: Broadcast address formats for the three classes.

Format of Broadcast Addresses

A broadcast address may vary depending on the class of the IP address. The following table lists the format of different broadcast addresses for different classes of octets w.x.y.z.

Class	Subnet Mask	Netmask/ Network Part	Host Part	Broadcast Address
A	255.0.0.0	w	x.y.z	w.255.255.255
B	255.255.0.0	w.x	y.z	w.x.255.255
C	255.255.255.0	w.x.y	z	w.x.y.255

Ports**Definition:**

On a network, a *port* is an access point to a logical connection. It serves as a channel through which information can be exchanged directly among networked computers. Many ports can operate simultaneously on a computer to provide services to different applications. A unique port number identifies the type of application that is sending or receiving data. It also informs the computer as to which application program running on the computer should process the data that is being sent or received through a particular port. Ports are identified by numbers between 0 and 65,536.

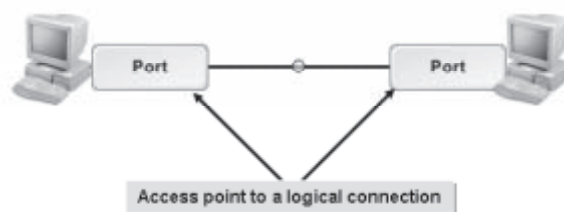
Example:

Figure 12-6: Transfer of data through ports on a network.

Allocation of Port Numbers

Just as several people live at the same address, such as in an apartment, multiple network applications may reside at the same IP address. In an apartment, suite numbers may be used in conjunction with the street address to identify which occupant should receive a mail. Similarly, the IP address along with a specific port number is allocated for different applications.

There is a scheme for identifying specific applications that share an IP address—and that is the addition of a port to the IP address. For example, a web server and an FTP server may both run on the same server, at 24.95.112.13. Web servers typically are set up to run on port 80, and FTP servers run on port 21. To identify the FTP server, you could use the address 24.95.112.13:21. The colon character separates the port address from the rest of the IP address.

Most servers enable the administrator to specify the port on which a service should run. The ability to specify the port number can be useful when multiple services, such as two web servers, are running on the same computer. One server may run on port 80 and the other on port 81.

Ports Allocated for Different Services

Ports can be allocated to different services based on the types of applications supported by a network. The `/etc/services` file contains a list of ports supported in Linux. Some of the common ports are listed in the table.

Port Number	Description
1	TCP Port Service Multiplexer (TCPMUX)
5	Remote Job Entry (RJE)
7	ECHO
18	Message Send Protocol (MSP)
20	File Transfer [Default Data] (FTP–Data)
21	File Transfer [Control] (FTP–Control)
22	Secure Shell Login (SSH)
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)
29	MSG ICP
37	Time
42	Host Name Server
43	WhoIs
49	Login Host Protocol
53	Domain Name System (DNS)
69	Trivial File Transfer Protocol (TFTP)
70	Gopher Services
79	Finger
80	HTTP
103	X.400 Standard
108	SNA Gateway Access Server

Port Number	Description
109	POP2
110	POP3
115	Simple File Transfer Protocol (SFTP)
118	SQL Services
119	Network News Transfer Protocol (NNTP)
123	Network Time Protocol
137	NetBIOS Name Service
139	NetBIOS Datagram Service
143	Interim Mail Access Protocol (IMAP)
150	NetBIOS Session Service
156	SQL Server
161	SNMP
179	Border Gateway Protocol (BGP)
190	Gateway Access Control Protocol (GACP)
194	Internet Relay Chat (IRC)
197	Directory Location Service (DLS)
389	Lightweight Directory Access Protocol (LDAP)
396	Novell Netware over IP
443	HTTPS
444	Simple Network Paging Protocol (SNPP)
465	Secure SMTP over TLS
546	DHCP Client
547	DHCP Server
631	Internet Printing Protocol (IPP)
1080	Socks
3306	MySQL

Port Ranges

The Internet Assigned Numbers Authority (IANA), an international agency, separates port numbers into three blocks: well-known ports, which are preassigned to system processes; registered ports, which are available to user processes and are listed as a convenience; and dynamic ports, which are assigned by a client operating system when there is a request for service.

Block	Description
Well-known ports	Port range: 0 to 1,023. These ports are preassigned for use by common, or well-known, services. Often, the services that run on these ports must be started by a privileged user. Services in this range include HTTP on TCP port 80, IMAP on TCP port 143, and DNS on UDP port 53.

Block	Description
Registered ports	Port range: 1,024 to 49,151. These ports are registered by software makers for use by specific applications and services that are not as well known as the services in the well-known range. Services in the registered port range include SOCKS proxy on TCP port 1080, Kazaa peer-to-peer file sharing on TCP port 1214, and Xbox Live on TCP and UDP port 3074.
Dynamic or private ports	Port range: 49,152 to 65,535. These ports are set aside for use by unregistered services and by services that need a temporary connection.

Network Interfaces

A *network interface* is a point of connection between two systems. It can be implemented using hardware or software. Different types of network interfaces are available.

Network Interface Type	Description
<i>Physical</i>	A network interface that is implemented using a hardware device. For example, an Ethernet interface (denoted by ethX, where X refers to the number of the interface) is set up using a Network Interface Card (NIC).
<i>Virtual</i>	A network interface that is implemented through software support. For example, a loopback interface (<i>lo</i>) simulates a network interface without the help of a physical device. It is used to test network connectivity and accuracy of data transmission by sending data back to the generating source address.

Network Interface Cards

Definition:

A *Network Interface Card (NIC)* is a small circuit board that enables a computer to connect to a network. A network interface is created between two or more computers using NICs. To connect to different networks—such as a wired or a wireless network—more than one NIC can also be installed on a computer. The different NICs connected to a system are numbered. A NIC is usually an internal or external adapter card that is installed into one of the system's expansion slots. NICs can even be built into the motherboard of the system, or connected through a USB port. After the NIC is installed, it has to be configured to connect to a particular network using the required network address and settings.

Example:

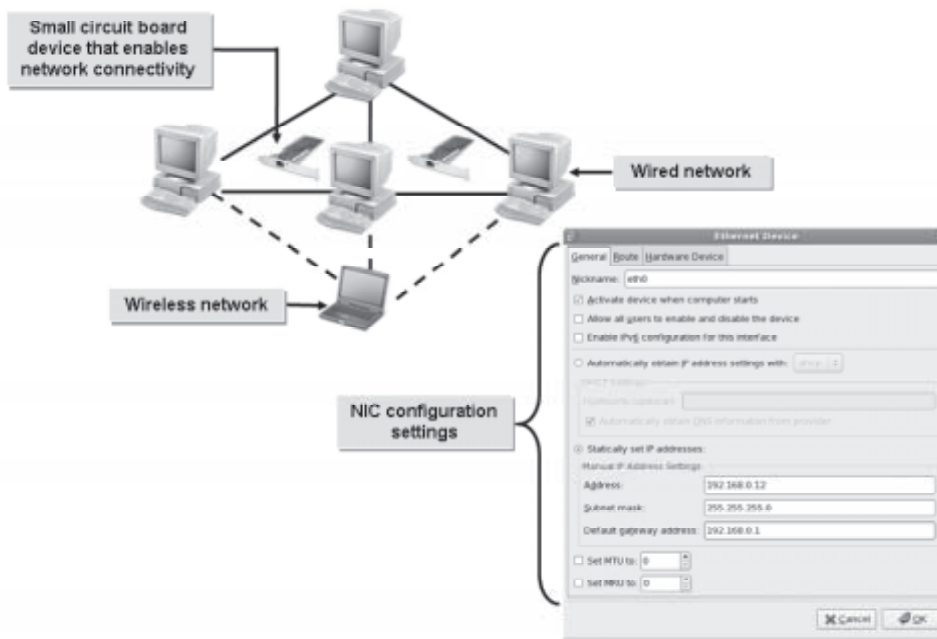


Figure 12-7: A NIC helps to connect computers and other devices on a network.

NIC Characteristics

NICs have some special characteristics that distinguish them from other types of adapter cards.

Characteristic	Description
Network connection port	Network adapter cards will have one or more ports that are configured to connect specifically to a given type of network cable. Some older cards had several types of ports so that they could connect to several different types of network cable. Network connections today are standardized and almost all use one port type.
Physical network address	Each network adapter has a globally unique <i>physical address</i> burned onto the card by the card manufacturer. The physical address uniquely identifies every individual card that connects to the network cable or media. For this reason, the physical address is also called the <i>Media Access Control (MAC) address</i> . MAC addresses are six bytes long. A typical MAC address may appear as 00-00-86-47-F6-65, where the first 3 bytes are the vendor's unique ID and the next 3 bytes uniquely identify that card's vendor.

Characteristic	Description
Status indicator lights	<p>Network adapters, including those built into most network devices, typically have one or more status indicator lights that can provide information on the state of the network connection.</p> <ul style="list-style-type: none"> • Most adapters have a <i>link light</i> that indicates if there is a signal from the network. If the link light is not lit, there is a problem with the cable or the physical connection. • Most adapters also have an <i>activity light</i> that flickers when packets are received or sent. If the light flickers constantly, the network may be overused or there may be a device generating network noise. • Some multi-speed adapters have a <i>speed light</i> to show whether the adapter is operating at 10 Mbps (Ethernet), 100 Mbps (Fast Ethernet), or 1,000 Mbps (Gigabit Ethernet). • Some types of equipment combine the functions of more than one light into <i>dual-color LEDs</i>. For example, a green flickering light may indicate normal activity, while an orange flickering light may indicate network traffic collisions.

The ifconfig Command

The *ifconfig* command is used for configuring network interfaces for Linux servers and workstations. It is also used to view the current TCP/IP configuration of a system, including the IP address and the netmask address.

```

root@localhost:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:C6:ED:E0
          inet addr:192.168.0.1  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fec6:ede0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5225659 errors:10 dropped:0 overruns:0 frame:0
          TX packets:1426965 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3301159228 (3.0 GiB)  TX bytes:116061331 (111.4 MiB)
          Interrupt:177 Base address:0x1400

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1358 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1358 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:3172706 (3.0 MiB)  TX bytes:3172706 (3.0 MiB)

root@localhost ~#
  
```

Figure 12-8: The output of the *ifconfig* command.

Syntax

The syntax of the *ifconfig* command is *ifconfig {interface name} {options | address}*.

ifconfig Command Options

The `ifconfig` command has many options. The most frequently used options are provided in the table.

Option	Function
<code>up</code>	Activates the interface.
<code>down</code>	Deactivates the interface.
<code>{address}</code>	Sets the IP address.
<code>netmask {address}</code>	Sets the network mask for the interface.
<code>dstaddr {address}</code>	Sets the remote IP address.

The ifconfig Command Interface

Linux provides an interface to the `ifconfig` command that makes configuration of a network device very simple. This interface is made up of the `ifup` and `ifdown` commands and two or more configuration files. The configuration files are the `/etc/sysconfig/network` file, which specifies the network configuration, and one or more files in the `/etc/sysconfig/network-scripts` directory, which contains device-specific networking information. For a system with a single Ethernet card, device-specific information is stored in the `/etc/sysconfig/network-scripts/ifcfg-eth0` file.



In older versions of Linux, the `/etc/HOSTNAME` or `/etc/hostname` file was used instead of the `/etc/sysconfig/network` file.

The `ifup` and `ifdown` commands are used to start and stop specific network devices, respectively. The syntax of these commands is `[command] {device name}`, where `[command]` is either `ifup` or `ifdown` and `{device name}` is the name of the device such as `eth0`, `eth1`, and so on.

Because the `ifup` and `ifdown` commands control only a single network device, it is often easier to use the `/etc/init.d/network` command with the `start` or `stop` parameters. This command starts (or stops) all network devices simultaneously.

The iwconfig Command

The `iwconfig` command is used for configuring wireless network interfaces for Linux servers and workstations. It is similar to the `ifconfig` command, except that it is used to set up and view the parameters of wireless network interfaces.

Syntax

The syntax of the `iwconfig` command is `iwconfig {interface name} {options | address}`.

The iwconfig Command Options

The `iwconfig` command has various options, which are provided in the table.

Option	Function
essid	Sets the ESSID, also called network name or domain ID, which is used to identify cells that are part of the same virtual network.
nwid/domain	Sets the network ID, which differentiates the wireless network from other networks and identifies nodes belonging to the same cell.
nick	Sets the nickname or the station name that is used by some wireless tools.
mode	Sets the operating mode of the device.
freq/channel	Sets the operating frequency or channel of the device.
ap	Registers the access point given by the address.
rate/bit	Sets the bit-rate.
txpower	Sets the transmit power.
sens	Sets the sensitivity threshold.
retry	Sets the maximum number of retries.
rts	Sets the size of the smallest packet for which the node sends Request To Send (RTS).
frag	Sets the maximum size for fragments that can be transferred.
key/enc	Sets the encryption or scrambling keys and security mode.
power	Sets power management parameters.
commit	Applies all pending changes.

Cells

A cell is a network zone covered under a tower or access point.

RTS

RTS is a signal sent by a communication device to a receiving device, to verify if the receiving device is ready to accept the data that is to be sent to it. For example, a modem sends an RTS to a computer before it transmits data.

Subnets

Subnets are used in large organizations, such as universities and corporations, where it is necessary to divide the network into smaller, more manageable segments. Subnets are logical subsections of a large network. Each segment requires its own network address and host identifiers and is treated as a subnet of the original network.

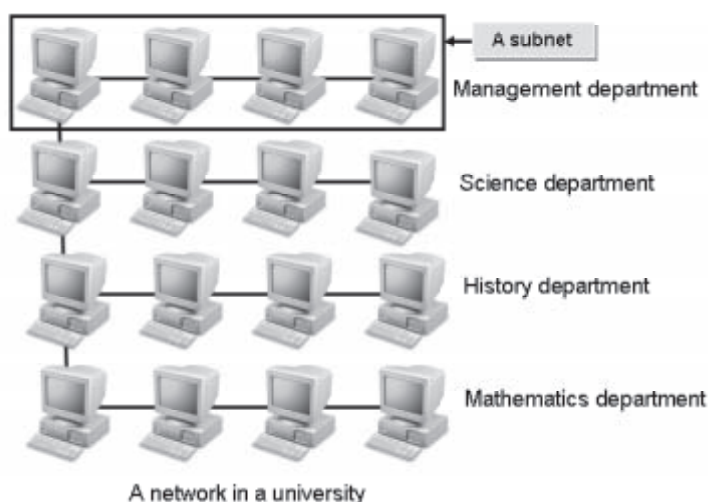


Figure 12-9: A subnet on a university network.

LDAP

Definition:

The *Lightweight Directory Access Protocol (LDAP)* is a communication protocol that defines the transport and format of messages used by a client to access the *directory service*. LDAP stores information in a directory in the form of a hierarchical tree structure. It authenticates users before they are allowed to query or modify information that resides in a directory. LDAP is run on TCP/IP networks.

Example:



Figure 12-10: A client accessing directory service through LDAP.

LDAPv3

LDAPv3 provides strong authentication and data security to Internet protocols using the *Simple Authentication and Security Layer (SASL)*. LDAPv3 controls extended operations and is internationalized through the use of Unicode. It provides secure transmission of data through the *Secure Socket Layer (SSL)*.

The Stand-Alone LDAP Daemon

The *Stand-alone LDAP Daemon (slapd)* is an LDAP directory service. The slapd allows users to create and provide their own directory service that can be connected to the global LDAP directory service. It supports different platforms and provides a certification-based authentication. It can be configured dynamically using LDAP, and

the configuration file `slapd.conf` is created in the `/etc/openldap` directory. The `slapd` directory service provides the features of data security, TCP wrappers, access control based on the LDAP authentication information, domain name and IP address, and high-performance database back-end. It also supports configuring multiple databases simultaneously, multi-threading, creating shadow copies of directory service, and providing LDAP proxy service.

The LDAP Process

The LDAP directory service is a client-server model that enables network clients to use the directory service available on servers. The following stages are involved with the LDAP process.

1. The LDAP client sends a request to access the directory service.
2. The LDAP server accepts the request and authenticates the user. If the user is valid, it allows the user to access the directory service. Otherwise, it returns an error message.
3. The user sends a request to the server to search for information.
4. The server processes the request. It sends either the result or a pointer where the information is available to the client.
5. And, the client uses the information sent by the server.

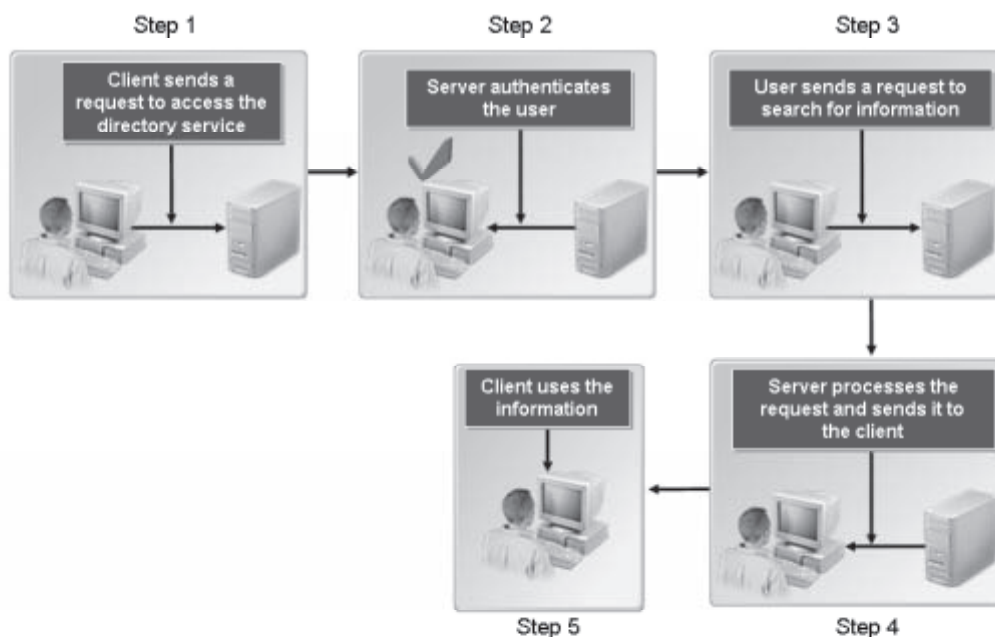


Figure 12-11: The different stages in the LDAP process.

How to Connect to a Network

Procedure Reference: Manually Configure a NIC

To manually configure a NIC:

1. Log in as root in the CLI.
2. To stop the network service, enter `service network stop`.
3. Enter `cd /etc/sysconfig/network-scripts`.



The `/etc/sysconfig/network-scripts/` directory contains various network scripts, such as `ifcfg-eth0`, that will be executed whenever a system starts up.

4. Enter `vi ifcfg-{device name}`.
5. Make the necessary changes in the file.
 - To change the booting protocol to static, change **BOOTPROTO=dhcp** to **BOOTPROTO=static** and press **Enter**.
 - To specify the IP address of the NIC, enter `IPADDR={IP address}`.
 - To specify the netmask address, type `NETMASK={netmask}`.
6. Save and close the file.
7. To restart the network service, enter `service network start`.

BOOTPROTO

BOOTPROTO is a variable that is used to specify the mode in which a NIC is configured. If **BOOTPROTO=static**, then the NIC will be configured manually. If **BOOTPROTO=dhcp**, then the NIC will contact the DHCP server to obtain the IP information.

Procedure Reference: Automatically Configure a NIC

To automatically configure a NIC:

1. Ensure that the DHCP server is configured and running. If necessary, check with your system administrator.



A DHCP server automatically allocates IP addresses to a client.

2. Log in as root in the CLI on a client system.
3. Enter `cd /etc/sysconfig/network-scripts`.
4. To open the device file, enter `vi ifcfg-{device name}`.
5. To change the booting protocol to dhcp, modify **BOOTPROTO=static** to **BOOTPROTO=dhcp**.
6. Save and close the file.
7. To restart the network service, enter `service network restart`.
8. If necessary, to check the network connectivity, enter `ping -{options} {destination IP address}`.

The pump and dhcpcclient Commands

The `pump` and `dhcpcclient` commands were used by older versions of Linux to get the IP address from the DHCP server. In the latest version, when you configure **BOOTPROTO=dhcp** in the `/etc/sysconfig/network-scripts/ifcfg-{device name}` file and restart the network service, it automatically obtains the IP address from the DHCP server.

The ping Command Options

The `ping` command is used to test network connectivity.

A few frequently used `ping` command options are described in the following table.

If You Need To	Use This <code>ping</code> Option
Ping the destination IP address for a specified number of times.	<code>-c {number}</code>
Ping the destination IP address at regular intervals.	<code>-i {number}</code>
Broadcast the ICMP packages for a specified network.	<code>-b {broadcast ID}</code>

The `ping` Command Restriction

Because the `ping` command generates ICMP traffic to the target hosts, a firewall can be set to block this traffic. Therefore, the `ping` command should be relied upon only when there are no known firewalls blocking the ICMP traffic.

Procedure Reference: Set a Temporary IP Address and Establish a Temporary Connection with Other Networks

To set a temporary IP address and establish a temporary connection with other networks:

1. Log in as root in the CLI.
2. To view the status of the active devices, enter `service network status`.
3. To view the details of all the configured devices, enter `ifconfig`.
4. To set a temporary IP address to the specified NIC device, enter `ifconfig -a eth{number} {new IP address}`.
5. If necessary, to revert to the original IP address, enter `service network restart`.

Procedure Reference: Add a New NIC

To add a new NIC:

1. Install the NIC.
 - a. Shut down the system and disconnect it from the power source.
 - b. Remove the cabinet.
 - c. Insert the NIC card in the free PCI slot.
 - d. Close the cabinet.
 - e. Connect the network cable to the NIC.
 - f. Connect to the power source and restart the system.
2. Log in as root in the CLI.
3. To navigate to the network-scripts directory, enter `cd /etc/sysconfig/network-scripts`.
4. To create a blank file, enter `touch ifcfg-eth{device name}`.
5. Enter `vi ifcfg-eth{device name}`.
6. To specify the device name, enter `DEVICE=eth{device name}`.

7. To automatically activate the device when the system starts, enter `ONBOOT=yes`.
8. Enter `BOOTPROTO=static`.
9. Enter `IPADDR={IP address}`.
10. Type `NETMASK={netmask}`.
11. Save and close the file.
12. To restart the network service, enter `service network restart`.

Procedure Reference: Disable a NIC


To disable a NIC:

1. Log in as root in the CLI.
2. Disable the NIC.
 - Enter `cd /etc/sysconfig/network-scripts` and delete the corresponding `ifcfg-eth{number}` file in the directory or;
 - Enter `ifdown eth{number}`.

 To enable the NIC, the `ifup eth{number}` command is given.

Delete a NIC

To delete any NIC device, delete the corresponding `ifcfg-eth{number}` file located in the `/etc/sysconfig/network-scripts/` directory.

 A NIC does not have to be physically removed from a system to delete it.

Procedure Reference: Configure a Wireless Network Interface Using the iwconfig Command

To configure a wireless network interface using the `iwconfig` command:

1. Log in as root in the CLI.
2. Specify the different parameters for the wireless interface.
 - To set the network name for the wireless device, enter `iwconfig {device number} essid {ess id} | {network name}`.
 - To set the network id for the wireless device, enter `iwconfig {device number} nwid {network id} | {domain id}`.
 - To specify the nickname for the wireless device, enter `iwconfig {device number} nickname {nickname}`.
 - To set the mode of the wireless device, enter `iwconfig {device number} mode {Ad-Hoc/Managed/Master/Repeater/Secondary/Monitor/Auto}`.
 - To set the frequency or channel for the wireless device, enter `iwconfig {device number} freq|channel {frequency value} | {channel number}`.
 - To set the access point for the wireless device, enter `iwconfig {device number} ap {access point id} | any | off`.

- To set the bit-rate for the wireless device, enter `iwconfig {device number} rate {bit rate}/auto`.
 - To set the encryption key for the wireless device, enter `iwconfig {device number} key {key value}`.
3. View the details of the configured wireless devices.
 - To view the details of all the configured wireless devices, enter `iwconfig`.
 - To view the details of a specific wireless device, enter `iwconfig {device number}`.
 4. To apply the changes, restart the network service.

Procedure Reference: Configure the LDAP Client

To configure the LDAP client:

1. Log in as root in the CLI.
2. To configure the LDAP client, enter `authconfig-tui` to use the **Authentication Configuration** utility.
3. In the **Authentication** section, select **Use LDAP Authentication**.
4. To go to the next screen, press **F12**.
5. If necessary, to transfer the encrypted password, on the **LDAP Settings** screen, check the **Use TLS** check box.
6. In the **Server** text box, type the LDAP server information.
7. In the **Base DN** text box, type the base distinguished name.
8. To finish and close the wizard, press **F12**.

Procedure Reference: Turn Off Network Services Not in Use

To turn off network services not in use.

1. Login as root in the CLI or GUI terminal.
2. To stop unnecessary network services, enter `service {network service name} stop`.
3. If necessary, to disable a network service at startup, enter `chkconfig {network service name} off`.

ACTIVITY 12-1

Connecting to a Network Manually



Before You Begin:

- 1. The system, srvB, is rebooted and the GUI login screen is displayed.
- 2. Log in to the GUI as root.
- 3. Switch to the first terminal of the CLI.

Scenario:

You are working as a system administrator in a startup company with only a few employees. Your responsibilities include setting up and configuring network connectivity in your organization. A new employee has joined your organization. You need to assign the employee a system and make it part of the existing network. The network configuration details of the system are as follows:

- IP address: 192.168.0.2
- Netmask: 255.255.255.0

What You Do	How You Do It
1. Identify the IP address of the system.	<div>a. Log in as root in the CLI.</div> <div>b. To view the inet addr 192.168.0X, enter ifconfig</div> <div> inet addr or InetAddress is a class that identifies the IP address of a host on a network.</div> <div> X represents the different host octet values provided by the DHCP server to all the students.</div> <div>c. Observe that the results contain details about Ethernet and loopback devices. In addition, observe that HWaddr is displayed along with the details about the received (RX) and transmitted (TX) packets.</div> <div>d. To clear the terminal screen, enter clear</div>

LESSON 12

2. Verify the IP address manually.
 - a. To change to the network-scripts directory, enter **cd /etc/sysconfig/network-scripts**
 - b. To open the device file, enter **vi ifcfg-eth0**
 - c. Observe that the default configuration of the NIC is displayed.
 - d. Verify that the **BOOTPROTO=static** line exists and press **Enter**.
 - e. Verify that the IP address for the NIC device is set as **IPADDR=192.168.0.X**
 - f. Verify that the netmask address for the NIC device is set as **NETMASK=255.255.255.0**
 - g. Close the file.
 - h. To restart the network service, enter **service network restart**
 - i. To clear the terminal screen, enter **clear**

 3. Test the network connectivity.
 - a. To check network connectivity, enter **ping -c 5 192.168.0.2**
 - b. Observe that the response from **192.168.0.2** is displayed five times with the **ttl** and **time**, which indicates that the network is functional. In addition, observe that the statistics section displays details about the number of packets transmitted and received, percentage of packet loss, and the total time taken.
 - c. To clear the terminal screen, enter **clear**
-
-

TOPIC B

Configure Routes

In the previous topic, you configured the IP settings for network interfaces. Routing allows you to manage data transmission traffic on networks. It enables data to be transmitted from a source to its destination through different routes. In this topic, you will configure routes.

Computers on a network interact with each other simultaneously at numerous instances. If one computer on a network communicates with many computers at the same time, and if the data transmission routes or communication paths are not configured, it may lead to a system crash due to flooding of information. Therefore, the routes for information transmission have to be configured to avoid collision in network traffic.

Routers

Definition:

A *router* is a networking device that connects multiple networks. Routers enable data to be exchanged among networks by examining and determining the best network path for data to travel. A router can be a dedicated device or can be implemented as a software application running on a network enabling device.

Example:

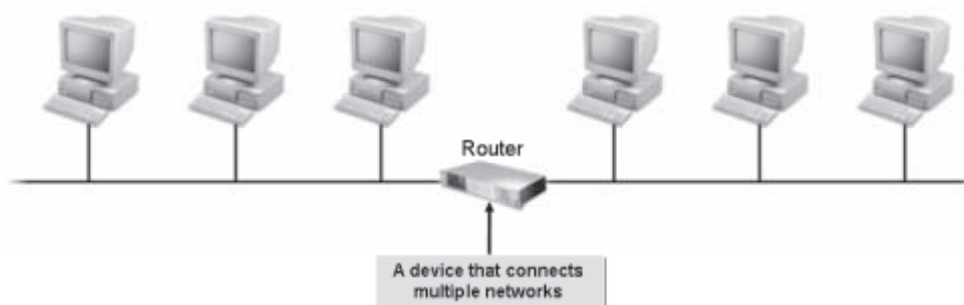


Figure 12-12: A router connecting two networks.

Routing

Definition:

Routing is the process of selecting the best route for moving data packets from a source to its destination on a network. To assist the process of routing, a router applies appropriate algorithms to generate and maintain an information base about network paths. It considers various metrics, such as the path bandwidth, path reliability, and communication costs, while evaluating the available network paths to determine the optimal route for forwarding a packet. Once the optimal route for a packet is assigned, packet switching is done to transfer the packet from the source host to the destination host.

Example:



Figure 12-13: *Example of routing on a network.*

Packets

A *packet* is a formatted unit of data being sent across a network. In addition to the user data, it comprises control information, such as the source and destination addresses, which are required to deliver the user data. A packet is also known as a *datagram*.

Packet-Switching Technology

Packet-switching technology is used for transmitting data among computers on a network. In a packet-switched network, a message is broken into packets, which are transmitted individually or switched to their required destination. During the process, each packet may follow a different path, but at the destination, the packets are reassembled to form the original message sent from the main destination. This technology ensures greater routing and transporting efficiency on a network. The Internet is a packet-switched network.

Benefits of Packet-Switched Networking

The benefits of a packet-switched network lie in the underlying technology of dividing a message to be sent over the Internet into packets. When data is transported in packets rather than in one big stream of data, the packets do not all have to move through the same path. Because the data is broken up into small packets, the packets can be sent across the Internet over various paths, eventually (in a fraction of a second) reaching their destination, where the packets can be reassembled into the original data. This means that one or more of the smaller networks, which make up the Internet, can go out of service without preventing the packets from ultimately reaching their destination, because the packets can simply take a different path to get there. If a few packets never reach their destination, they can be resent over a different path.

If files were not broken up into smaller packets, the entire file will have to be resent if any part of it did not reach the destination intact. Having multiple paths and breaking up files into small packets increase the reliability of the network.

Routing Tables

Routers exchange information with each other by building a table of network addresses. This information base is called a *routing table*. Routers refer to this table to determine where to forward the packets. If a router that is attached to four networks receives a packet from one of these networks, it will determine which of the other three networks is the best route to send the packet so that it could reach its destination quickly.

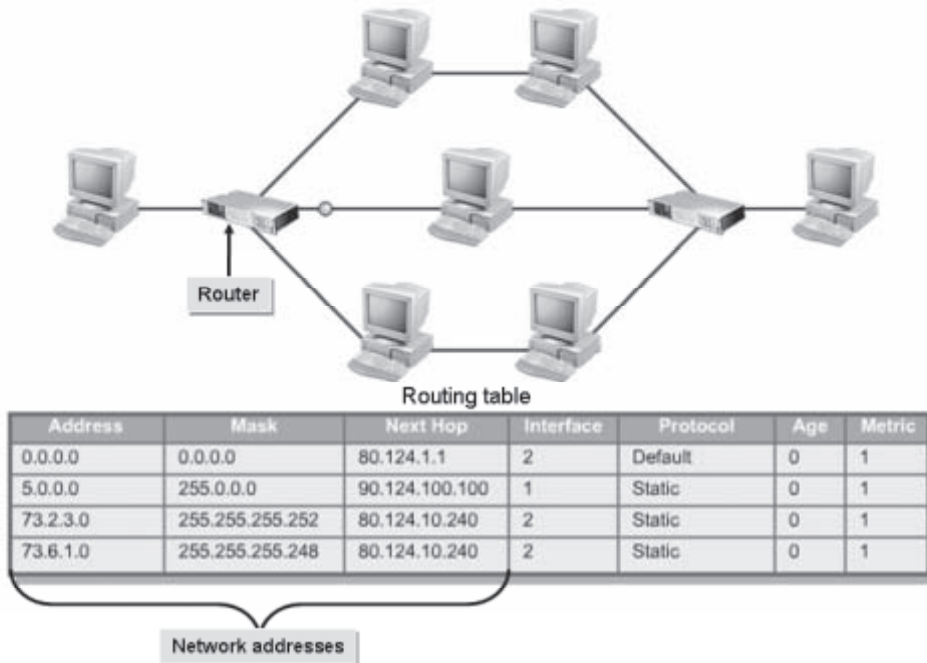


Figure 12-14: A routing table that comprises network addresses.

The route Command

The `route` command manipulates the kernel's IP routing tables. Its primary use is to set up static routes to specific hosts or networks. When the `add` or `del` option is used, the `route` command modifies the routing tables. Without these options, the `route` command displays the contents of the routing tables.

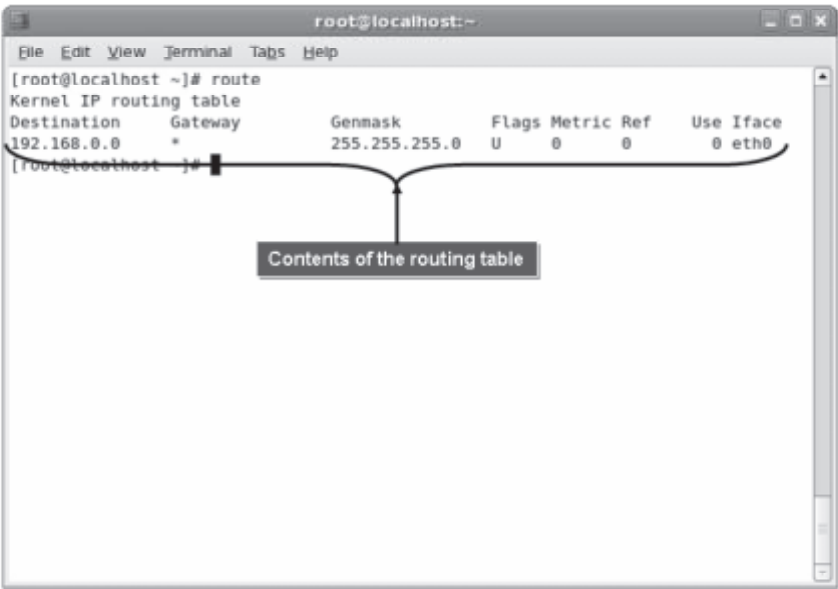


Figure 12-15: The output of the route command.

Routing Examples

The table displays a few routing examples.

Command	Description
<code>route add -net 127.0.0.0</code>	Adds the normal loopback entry using netmask 255.0.0.0 (class A net, determined from the destination address) and associated with the lo device, assuming this device was previously set up correctly with ifconfig.
<code>route add -net 192.56.76.0 netmask 255.255.255.0 dev eth0</code>	Adds a route to the network 192.56.76.x via eth0. The Class C netmask modifier is not really necessary here because 192.* is a Class C IP address. The word “dev” can be omitted here.
<code>route add default gw mango-gw</code>	Adds a default route, which will be used if no other route matches. All packets using this route will be gatewayed through mango-gw. The device that will actually be used for that route depends on how mango-gw can be reached—the static route to mango-gw will have to be set up before.
<code>route add -net 192.57.66.0 netmask 255.255.255.0 gw ipx4</code>	Adds the net 192.57.66.x to be gatewayed through the former route to the SLIP interface.
<code>route add -net 10.0.0.0 netmask 255.0.0.0 reject</code>	Installs a rejecting route for the private network 10.x.x.x.

Gateways

Definition:

A *gateway* is a device, software application, or system that converts data between incompatible systems. Gateways can translate data among different operating systems, email formats, or networks. It can link two dissimilar networks, which operate on varying protocols, enabling them to communicate with each other and exchange information.

Example:

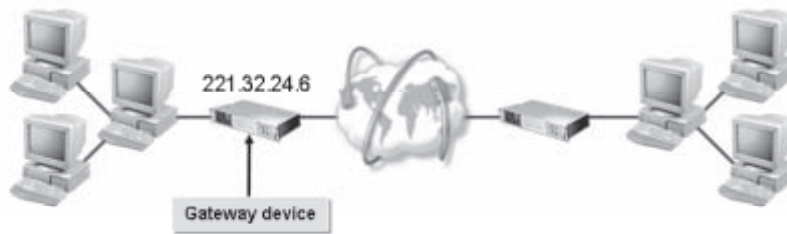


Figure 12-16: A gateway device linking dissimilar networks.

The Default Gateway

The *default gateway* is the gateway that acts as a network segment's access point to all other external networks and the Internet. The IP address assigned to the default gateway router is called the *default gateway address*. It is important because this address is configured as the access point to all the computers on that network segment. It provides an access path for packets in and out of the network segment.

The traceroute Command

The `traceroute` command is used to print the route that packets take to reach their destination. This is useful in troubleshooting some network or Internet connectivity problems. There are several options for the `traceroute` command.

Option	Description
<code>-d</code>	Sets the socket level debug option.
<code>-n</code>	Prints hop addresses numerically.
<code>-i {interface}</code>	Specifies the interface through which traceroute should send packets.
<code>-g {gateway}</code>	Specifies a source route gateway.
<code>-r</code>	Bypasses the normal routing tables and sends the packets directly to a host on an attached network.
<code>-w {waittime}</code>	Sets the time, in seconds, to wait for a response to a probe.



Like `traceroute`, `tcpdump` is another network monitoring package that can be installed on a Linux system.

The netstat Command

The `netstat` command displays statistics about a network, including socket status, interfaces that are auto-configured, memory statistics, and routing tables. With no arguments, the default `netstat` command displays open sockets.

Some of the frequently used `netstat` command options are described in the following table.

Option	Displays
-r or --route	The kernel routing tables.
-g or --groups	The multicast group membership.
-i or --interface or --interface={iface}	A table of all network interfaces or the specified interface.
-M or --masquerade	A list of masqueraded connections.
-s or --statistics	A summary of statistics for each protocol.
-e or --extend	Additional details.

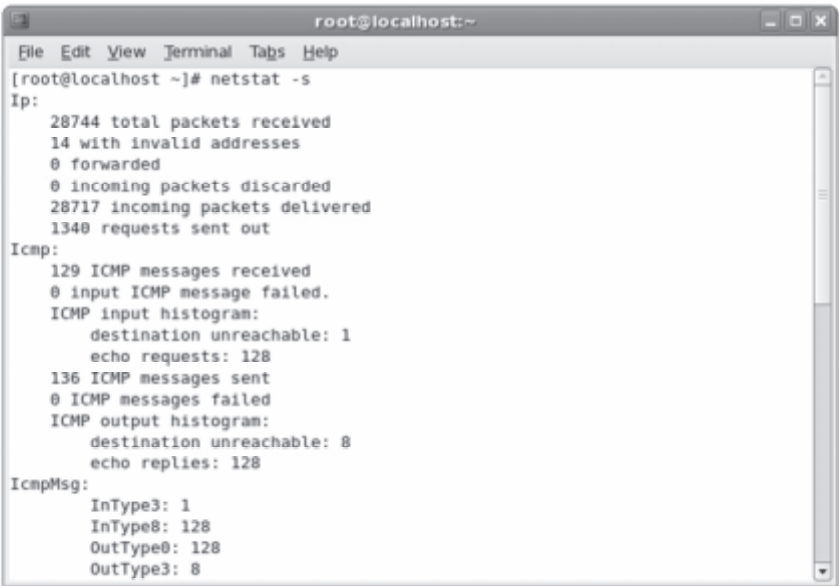


Figure 12-17: The `netstat` command displaying a summary of statistics for each protocol.

How to Configure Routes

Procedure Reference: Configure a Route for the IPv4 Address

To configure a route for the IPv4 address:

1. Log in as root in the CLI.
2. To add a static route, enter `ip route add {network part of IPv4 address}/{length} via {gateway IPv4 address}`.
3. Make the static route persistent.

- a. To stop the network interface service, enter `ifdown eth{device number}`.
 - b. To open the network-scripts directory, enter `cd /etc/sysconfig/network-scripts`.
 - c. To open the NIC configuration file, enter `vi route-eth{device number}`.
 - d. To configure the route, specify *{network part of IPv4 address}/{length}* via *{gateway IPv4 address}*.
 - e. Save and close the file.
 - f. To start the network interface service, enter `ifup eth{device number}`.
4. View the updated routing table.
 - Enter `route` or;
 - Enter `netstat -r` or;
 - Enter `ip route`.

The ip Command

The `ip` command is used to show or manipulate routing, policy routing, devices, and tunnels. The syntax of the `ip` command is `ip [options] {object} {command | help}`.

Procedure Reference: Check the IPv4 Connectivity

To check the IPv4 connectivity:

1. Log in as root in the CLI.
2. Check the IPv4 connectivity.
 - To check the connectivity between the two systems, enter `ping [options] {IPv4 or hostname of destination system}`.
 - To view the network path to the destination system, enter `traceroute [options] {IPv4 or hostname of destination system}`.
 - To check the connectivity of the network path to the destination system, enter `mtr [options] {IPv4 or hostname of destination system}`.
 - To trace the network path and calculate the associated Maximum Transmission Unit (MTU) to the destination system, enter `tracepath [options] {IPv4 or hostname of destination system}`.



`mtr` is a network diagnostic utility that combines the functionality of the `traceroute` and `ping` commands.

Procedure Reference: Configure the Default Gateway for the IPv4 Address

To configure the default gateway for the IPv4 address:

1. Log in as root in the CLI.
2. Configure the default gateway.
 - Configure the default gateway globally.

- a. To open the sysconfig directory, enter `cd /etc/sysconfig`.
- b. To open the network settings file, enter `vi network`.
- c. Switch to insert mode.
- d. To specify the IP address of the gateway, enter `GATEWAY={IPv4 address of the gateway system}`.
- e. Save and close the file.
- f. To stop the device, enter `ifdown eth{device number}`.
- g. To start the device, enter `ifup eth{device number}`.
- Configure the default gateway for each NIC.
 - a. To stop the network interface service, enter `ifdown eth{device number}`.
 - b. To open the network-scripts directory, enter `cd /etc/sysconfig/network-scripts`.
 - c. To open the NIC configuration file, enter `vi ifcfg-eth{device number}`.
 - d. To set the IP address of the gateway, specify `GATEWAY={IPv4 address of the gateway system}`.
 - e. Save and close the file.
 - f. To restart the network interface service, enter `ifup eth{device number}`.

Procedure Reference: Configure a Route for the IPv6 Address

To configure a route for the IPv6 address:

1. Log in as root in the CLI.
2. To add a static route, enter `ip -6 route add {network part of IPv6 address}/{length} via {gateway IPv6 address}`.
3. Make the static route persistent.
 - a. To stop the network interface service, enter `ifdown eth{device number}`.
 - b. To open the network-scripts directory, enter `cd /etc/sysconfig/network-scripts`.
 - c. To open the file containing route settings, enter `vi route6-eth{device number}`.
 - d. To configure the route, specify `{network part of IPv6 address}/{length} via {gateway IPv6 address}`.
 - e. Save and close the file.
 - f. To start the network interface service, enter `ifup eth{device number}`.
4. To view the updated routing table, enter `ip -6 route`.

Procedure Reference: Check the IPv6 Connectivity

To check the IPv6 connectivity:

1. Log in as root in the CLI.

2. Check the IPv6 connectivity.
 - To check the connectivity between the two systems, enter `ping6 [options] {IPv6 or hostname of destination system}`.
 - To view the network path to the destination system, enter `traceroute6 [options] {IPv6 or hostname of destination system}`.
 - To trace the network path and calculate the associated MTU to the destination system, enter `tracepath6 [options] {IPv6 or hostname of destination system}`.

Procedure Reference: Configure the Default Gateway for the IPv6 Address

To configure the default gateway for the IPv6 address:

1. Log in as root in the CLI.
2. To open the sysconfig directory, at the command prompt, enter `cd /etc/sysconfig`.
3. To open the network settings file, enter `vi network`.
4. Switch to insert mode.
5. To set the IP address of the gateway, specify `IPV6_DEFAULTGW={IPv6 address of the gateway system}`.
6. Save and close the file.
7. To stop the device, enter `ifdown eth{device number}`.
8. To start the device, enter `ifup eth{device number}`.

ACTIVITY 12-2

Configuring Routes

Before You Begin:

1. On srvB, you logged in as root in the CLI.
2. The first terminal is displayed.

Scenario:

One of your tasks as a system administrator was to configure network connectivity and IP addresses on a new system. Now, you need to configure the router settings to connect to other computers on the network.

LESSON 12

What You Do	How You Do It
1. Specify the router settings for automatic configuration of routes.	<ol style="list-style-type: none">To stop the network interface service, enter ifdown eth0To configure the default gateway, enter cd /etc/sysconfigTo open the file, enter vi networkTo go to the last line, press Shift+G.To switch to insert mode and move to a new line, press O.On the new line, type GATEWAY=192.168.0.2To switch to command mode, press Esc.Save and close the file.
2. Start the network interface and view the updated routing table.	<ol style="list-style-type: none">To start the network interface service, enter ifup eth0To view the IP address, enter ifconfigObserve that the IP address of srvB is 192.168.0.X.To view the updated routing table, enter routeObserve that the gateway address is displayed.To clear the terminal screen, enter clear

TOPIC C

Configure Client Network Services

In the previous topic, you configured routers for transmission of data among computers on a network. The settings of the system determine the network resources that it can access. In this topic, you will configure network services on client systems.

On large networks, network administrators will have difficulty in assigning IP addresses to systems manually. It is easier for network users to remember system names instead of IP addresses. Without proper identification, a system will not have access to network resources. As a system administrator, you need to ensure that the IP address is properly assigned to the system and network users can use the system name to communicate with other network systems.

DHCP

The *Dynamic Host Control Protocol (DHCP)* allocates IP addresses on an as-needed basis to a client. Instead of using static IP addressing, DHCP leases a temporary IP address to the client for a specified period of time.

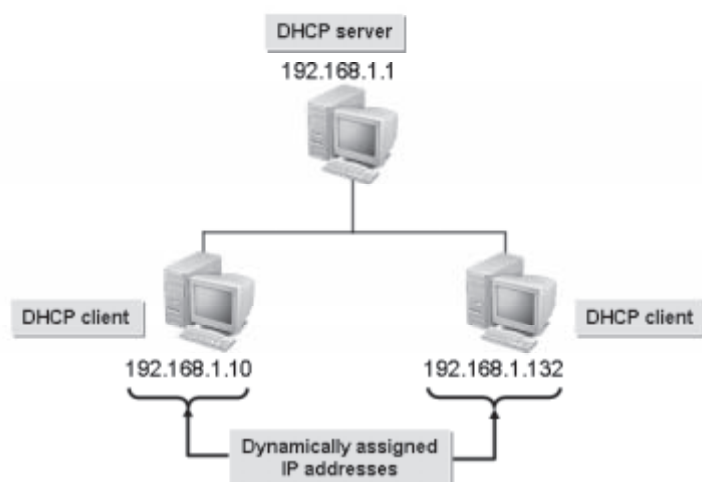


Figure 12-18: A DHCP server assigning IP addresses to clients.

DHCP Clients

A DHCP client is a system that gets network connectivity information from the DHCP server.

DHCP Components

There are a variety of components in a DHCP implementation, but not all have to exist in every DHCP setup.

Component	Description
Options	Items, in addition to an IP address and subnet mask, that may be assigned to client systems such as default gateways and DNS server addresses.
Scope	The range, or pool, of addresses for a given subnet that a DHCP server will assign.
Reservation	An option whereby a client consistently gets the same configuration information after every initialization.
Lease	The process of assigning an IP address and its associated options to a client for a finite or infinite period of time.

Allocation of IP Addresses

IP addresses can be allocated in three different ways.

Type of Allocation	Description
Manual	To allocate IP addresses manually, the administrator has to visit each host. Hosts can be either workstations or servers. Smaller organizations that have plenty of IP addresses for workstations and servers often use this method. When IP address assignments need to change, this method requires higher maintenance by the administrator.
Automatic	By using automatic allocation, the DHCP server assigns a permanent IP address to the host. The administrator need not visit each system. While this method reduces the amount of administrative time, it requires an adequate supply of IP addresses.
Dynamic	By using dynamic allocation, the DHCP server assigns a temporary IP address to the host. The administrator need not assign the IP addresses, and a limited number of IP addresses serves a larger organization. When a workstation boots, it requests an IP address from the DHCP server along with other information, such as the DNS server IP address, the gateway IP address, and the subnet mask. The DHCP server takes an address from a pool of IP addresses and gives it to the workstation to use temporarily. The administrator can configure how long the address is leased.

The DHCP Process

DHCP is a system-V service that handles client requests on a network and allocates IP addresses. The service gets activated on the system by installing the DHCP package. The DHCP process can be divided into a number of phases.

1. In the IP request phase, a client broadcasts the IP address request to the DHCP server.
2. In the IP release phase, the DHCP server receives the request and processes it. It responds to the request by sending the IP address, the subnet mask, the duration of lease, and the IP address of the DHCP server to the client.
3. In the client acceptance phase, the client accepts the information and broadcasts it to the network server so that the server ensures that the IP addresses used by the clients are unique.
4. In the server verification phase, the server sends a message to the client stating that it received the acceptance and the client is configured to use TCP/IP.
5. And, in the lease renewal phase, when half of the lease time has expired, the client sends a request to the server to extend the lease time or sends a request for a new IP address.

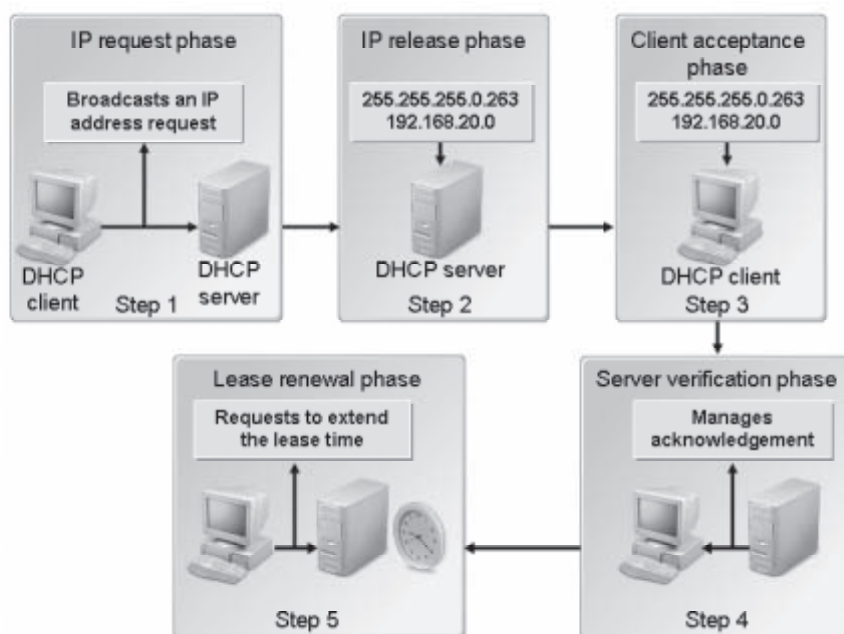


Figure 12-19: Different phases of the DHCP process.

The DNS

The *Domain Name System (DNS)* is a distributed, hierarchical database system that maintains information about domain names and their equivalent IP addresses on a network. It uses this information to translate a fully qualified domain name into its numeric IP address or vice versa. IP addresses are used by networked computers to locate, connect, and communicate with each other. The DNS translates IP addresses to their corresponding domain names. It works like a central system ensuring that there are no duplicate domain names and IP addresses on the network.

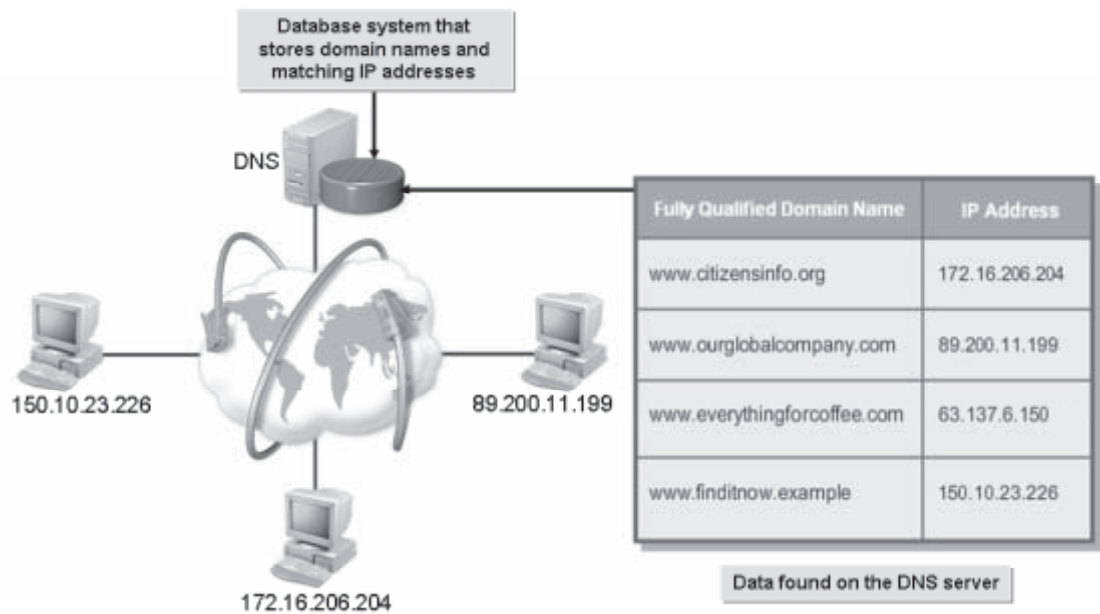


Figure 12-20: Allocation of domains using the DNS.

DNS Utilities

Various utilities are used to resolve DNS hostnames. Some of the resolving utilities are `dig`, `host`, and `nslookup`.

Domain Names

Definition:

A *domain name* is a label given to a *domain*, which is a node in the hierarchical structure of data stored in the DNS. It is the concatenation of all labels from the node to the root node. A domain name is represented by a string, and each node is separated by a period. Each domain name is unique within its parent domain.

Example:

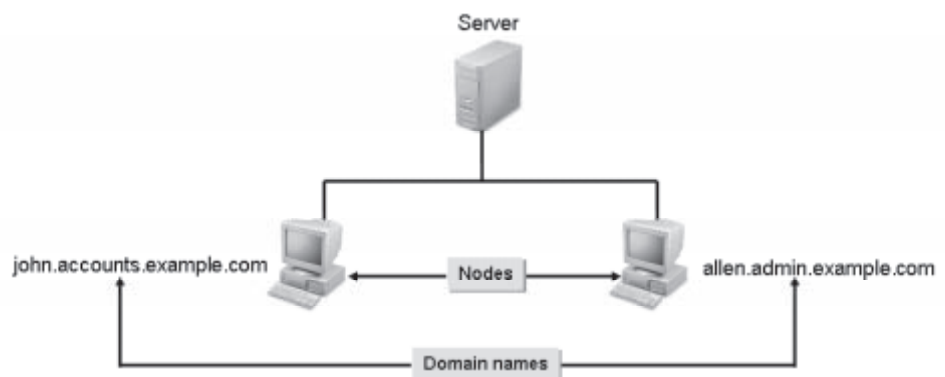


Figure 12-21: Assigning domain names to systems.

Subdomains

A subdomain is a part of a larger domain name. A DNS hierarchy comprises a root-level domain, followed by top-level domains, second-level domains, and subdomains. Each top-level domain contains subdomains, which are referred to as child domains.

The FQDN

A *Fully Qualified Domain Name (FQDN)* is a method by which systems are uniquely identified on the worldwide network. A complete domain name consists of a hostname, second-level domain, and the top-level domain.

Zones

Definition:

A *zone* is a point of delegation in a DNS tree structure that maps to a domain. A zone can map to an entire domain with all of its child domains or to a specific portion of a domain. Each zone will have one authoritative name server or one or more secondary name servers. There are two types of zones: forward and reverse.

Example:

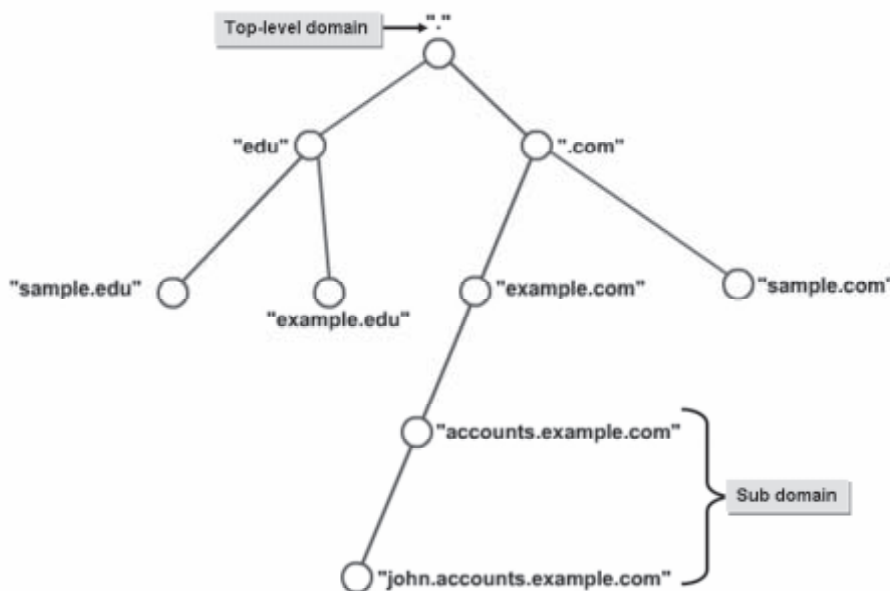


Figure 12-22: Delegation of domains using zones.

The Forward and Reverse Zones

The two main DNS zones are forward and reverse zones.

Zone	Description
Forward zone	A zone that is used for mapping hostnames to IP addresses. It contains information on the time allocated for the DNS server to get updated.

Zone	Description
Reverse zone	A zone that is used for mapping IP addresses to hostnames. A reverse zone can be used to resolve the IP address of a domain to trace unauthorized users.

The Domain Name Resolution Process

The process of domain name resolution involves a number of phases.

- 1. The DNS query containing the domain name is sent by an application to the resolver, requesting an IP address.
- 2. The resolver searches its cache for matching domain names. If any entry is found, then the respective IP address is forwarded to the client application. In case no entries are found, then the query is forwarded to the name server.
- 3. The name server, if authoritative for the zone, sends the reply to the resolver. If the name server is nonauthoritative, then the secondary name server forwards the query to the primary or authoritative name server, which sends the reply to the resolver.
- 4. And, the resolver then resolves the IP address and sends the reply to the client.

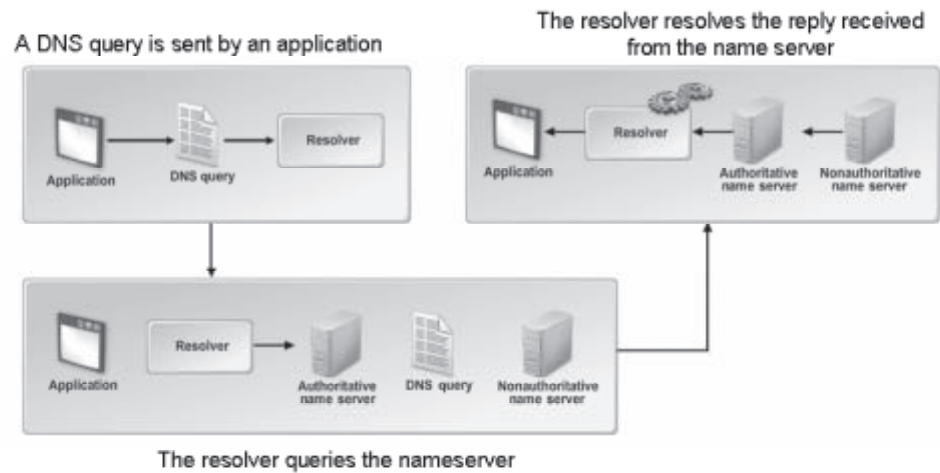


Figure 12-23: The various steps in the domain name resolution process.

The dig Utility

The `dig` utility interacts with name servers and displays the results to users. It may be configured to query a single name server or multiple name servers in the form of batches. It references the `/etc/resolv.conf` file for the list of name servers to be queried.

Various options can be used to configure the `dig` utility based on user requirements. Some of the frequently used command options are listed in the table.

Command Option	Description
-b	Sets the source IP address of the query. The utility will query name servers using this IP address.

Command Option	Description
<code>-f {file name}</code>	Enables the utility to query name servers based on the processes listed in the specified file.
<code>-p {port#}</code>	Specifies the port to be used to send queries.
<code>-4</code>	Forces the utility to use only the IPv4 protocol for querying.
<code>-6</code>	Forces the utility to use only the IPv6 protocol for querying.
<code>-t {query type}</code>	Sets the query type. Some of the valid query types are <code>soa</code> , <code>axfr</code> , <code>ixfr</code> , and <code>mx</code> .

Various query options can be used to configure the `dig` utility based on user requirements. Some of the frequently used query options are listed in the table.

Query Option	Enables You To
<code>+tcp</code>	Set the resolver to use the TCP service to query the name server.
<code>+domain={somename}</code>	Create a search list for the desired domain.
<code>+search</code>	Configure the resolver to use the search list specified in the <code>/etc/resolv.conf</code> file or through the <code>+domain</code> option.
<code>+nssearch</code>	Configure the resolver to search for name servers based on the zones in which they are defined.
<code>+identify</code>	Display the IP address and port number of the name server that answers the query.
<code>+trace</code>	Trace the DNS query for root name server information from the <code>/etc/resolv.conf</code> file.

Syntax

The syntax of the `dig` utility is `dig [options] {query options} {Fully Qualified Domain Name | IP address}`.

The host Utility

The `host` utility is a DNS lookup utility, similar to the `dig` utility. It is used to convert system names to IP addresses and vice versa. The `host` utility has various options.

Option	Enables You To
<code>{name}</code>	Set the domain name to be looked up by the <code>host</code> utility.
<code>-t {query type}</code>	Set the type of query to be sent to the name server.
<code>-W {seconds}</code>	Set the time the resolver must wait for a reply before quitting.
<code>-s</code>	Force the resolver to terminate the querying process once it fails without retrying.

Syntax

The syntax of the `host` utility is `host [options] {FQDN | IP address}`.

The nslookup Utility

The `nslookup` utility is used to query name servers over the Internet and check whether the name-to-IP address mapping is correct in the DNS configuration files. It operates in two modes—interactive and noninteractive. Interactive mode allows a client to query the name server for specific information. Noninteractive mode displays only standard information on the host.

Syntax

The syntax of the `nslookup` command is `nslookup {host name or FQDN}`.

Resolver Files

Various files are used to configure resolvers for resolving domain names and hostnames.

File	Description
The <code>hosts</code> file	The <code>/etc/hosts</code> file contains the hostname to IP address mapping information for systems on a network. In older versions of Linux, the <code>/etc/networks</code> file was used for this purpose.
The <code>host.conf</code> file	The <code>/etc/host.conf</code> file contains information on how the hostname lookups are to be performed. For example, if the <code>/etc/host.conf</code> file contains the line “ <code>order hosts,bind</code> ,” the hostname lookup will be performed first in the local <code>/etc/hosts</code> file and then in the DNS. The default entry in the <code>/etc/hosts</code> file is “ <code>order hosts,bind</code> .”
The <code>nsswitch.conf</code> file	The <code>/etc/nsswitch.conf</code> file, or the name server switch configuration file, contains information about each and every database and the order in which they work. The first column contains information about the database and ends with a colon; the remaining columns specify the order in which the database should use the service. For example, in the file entry <code>hosts: files dns</code> , <code>hosts</code> refers to the <code>hosts</code> database. This means that the host entries in the local files will have higher priority than the entries in the DNS server. In case the hostname entries are not found in the local files, the search will continue in the DNS.

File	Description
The resolv.conf file	The /etc/resolv.conf file, or the resolver configuration file, is a set of routines in the C library that provide access to the Internet DNS. The resolver configuration file contains a list of keywords with values that are read by the resolver routines, the first time they are invoked by a process. The three different configuration options are name server, domain, and search.

The named.conf File

Definition:

The *named.conf* file is a user-defined configuration file that is used to manage the BIND service. This file is invoked when the named service starts. It contains statements and comments. Statements define zone settings and comments contain messages or descriptions about the statements inside a file. Comments can be either a single-line or multi-line text.

 Single-line comments start with // and multi-line comments start with /* and end with */.

Example:

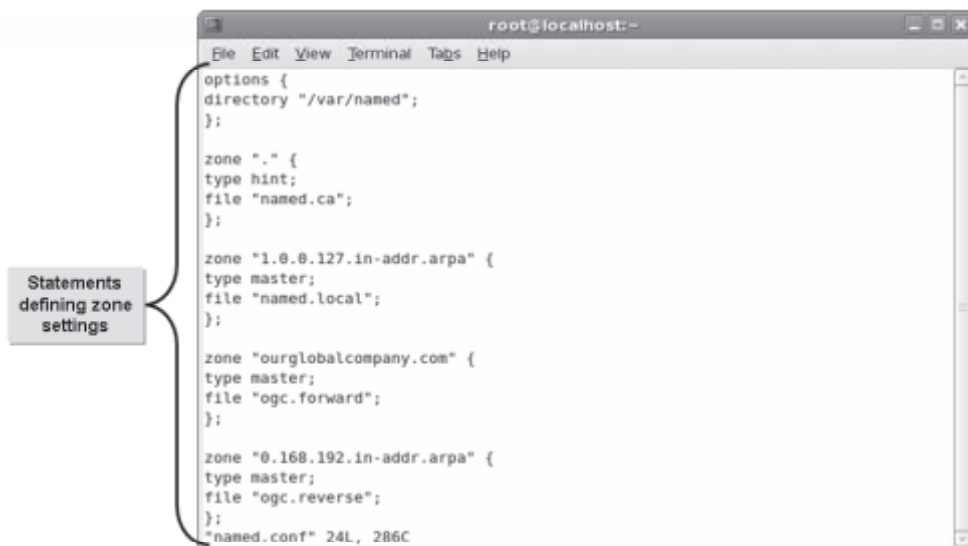


Figure 12-24: Various declarations in the *named.conf* file.

DNS Resource Records

A *DNS resource record* defines parameters for a zone. It contains five components: the fully qualified domain name, the TTL, the record class, the record type, and the record data. The format of a resource record is defined by the Request for Comments (RFC). The record data in a resource record depends on the record type.

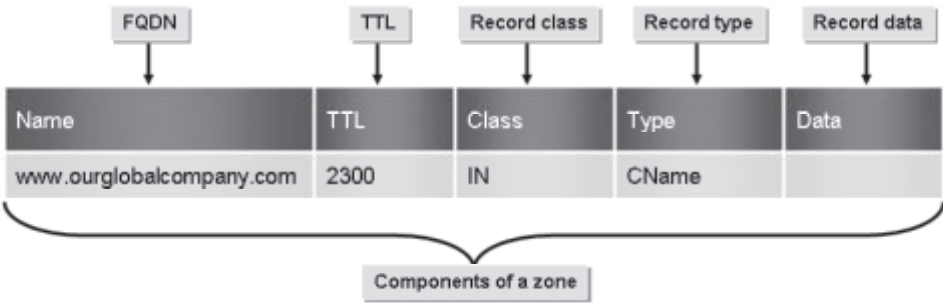


Figure 12-25: Interpretation of a DNS resource record.

Various DNS records and the format used for each are given in the table.

DNS Record	Description
SOA	The Start Of Authority (SOA) record is used to specify information about a zone in the string of fields format. The SOA record tells the server to be authoritative for the zone. Each zone will contain only one SOA record. The format of an SOA record is: @ IN SOA <i>primary nameserver</i> { <i>hostmaster email</i> }{ <i>serial number</i> }{ <i>time to refresh</i> }{ <i>time to retry</i> }{ <i>time to expire</i> }{ <i>minimum TTL</i> }).
NS	A Name Server (NS) record is used to define the authoritative name server for a specific zone. The format of the NS record is IN NS { <i>nameserver</i> }. The name server should be an FQDN. It can either be a primary server or a slave server.
A	An Address (A) record is used to assign an IP address to a name. The format of the A record is { <i>hostname</i> } IN A { <i>IP address</i> }. The IP address should not be terminated with a period (.). If the hostname is omitted, the A record will point to the default IP address at the top of the namespace.
PTR	The Pointer (PTR) record is used for reverse name resolution mapping. It is used in the reverse map zone files to map an IP address to a name. The format of the PTR record is { <i>last IP digit</i> } IN PTR { <i>FQDN of system</i> }. The { <i>last IP digit</i> } specifies the last number in an IP address, which should point to a particular system’s domain name. The PTR record should always end with a period. For example, 253 IN PTR srvA.example.com.

DNS Record	Description
MX	A Mail eXchange (MX) record is used to specify the relative preference of mail servers for a zone. The MX record format is <code>IN MX {priority value} {mail server name}</code> . The highest priority value is 0, which is assigned to a host where the mail is destined. Two hosts can have the same priority to distribute mail equally between them. Any number of MX records can be defined for a domain.
CNAME	A Canonical Name (CNAME) record is used to map an alias name to the real name. The CNAME record is also referred to as an alias record. The format of the CNAME record is <code>{alias name} IN CNAME {real name}</code> . CNAME records are generally used to point to another domain.
TXT	A Text (TXT) record is used to map text with a hostname. It is used to validate genuine email sources from a domain.

How to Configure Client Network Services

Procedure Reference: Configure the DHCP Client

To configure the DHCP client:

1. Log in as root in the CLI.
2. To open the device file, enter
`vi /etc/sysconfig/network-scripts/ifcfg-ethDevice name`.
3. Verify that `BOOTPROTO=dhcp`.
4. Save and exit.
5. To apply the settings, enter `service network restart`.
6. To verify that the system has received an IP address, enter `ifconfig`.



`dhclient` is a utility that allows you to configure one or more network services with the DHCP protocol. `dhclient` will assign a static address if the protocol fails.

Procedure Reference: Configure the DNS Service

To configure the DNS service:

1. Log in as root.
2. To use the `named.cachingnameserver.conf` file as a template, enter
`cp /etc/named.caching-nameserver.conf /etc/named.conf`.
3. Configure the DNS.
 - a. Specify the global configuration options.
 - b. Add zone statements for the root, loopback domain, and forward and reverse zones.
 - c. Create forward and reverse zone files.

4. To check the named syntax, enter `named-checkconf -f /etc/named.conf`.
5. Start the named service.
 - a. To start the named daemon, enter `service named start`.
 - b. If the named service is already running, to reload the named daemon, enter `service named reload`.
 - c. To reload the zone files, enter `rndc reload`.
 - d. To start the named service at system startup, enter `chkconfig named on`.

ACTIVITY 12-3

Configuring the DHCP Client Service

Before You Begin:

1. `srvA` is rebooted and the GUI login screen is displayed.
2. Switch to the first terminal of the CLI.
3. Log in as root.
4. To install the DHCP packages, at the command line, enter `yum localinstall /rhelsource/Server/dhcp*`.
5. To proceed with the installation, enter `y`.
6. Clear the terminal screen.

Before You Begin:

1. Switch to the system labeled `srvB`.
2. You are logged in to the GUI as root and the terminal window is displayed.

Scenario:

Your IT manager has defined the network layout planned for a new branch of your organization, OGC Systems. The network will include two Linux servers, (`srvA` and `srvB`), and 150 workstations. The DHCP service is installed on `srvA` for which the IP address 192.168.0.1 has been manually configured. You need to configure DHCP so that `srvB` and the workstations dynamically receive IP addresses from `srvA`. From the network policy documentation, you find that the IP addresses to be assigned can range from 192.168.0.25 to 192.168.0.200.

What You Do	How You Do It
1. Modify the network device setting to obtain address from the DHCP server.	<ol style="list-style-type: none"> a. To open the network configuration utility, in the terminal window, enter system-config-network-tui b. To edit the device parameters, in the Select Action dialog box, press Enter. c. To edit the device setting, verify that the NIC, eth0, is selected and in the Select A Device dialog box, press Enter. d. To move the cursor to the Use DHCP check box, in the Devernet Configuration dialog box, press the Down Arrow key two times. e. To check the Use DHCP check box, press the Spacebar. f. To apply the settings, press Tab and then press Enter. g. To save the device setting, press Tab and press Enter. h. To save the device setting, in the Select Action dialog box, press Tab and press Enter.
2. Check whether the DHCP settings have taken effect.	<ol style="list-style-type: none"> a. To request the DHCP server for an IP address, enter service network restart b. Observe that the network interfaces are shutdown and are started again and the IP information for eth0 is determined successfully. c. To verify that the IP address 192.168.0.X/24 has been assigned to srvB, enter ip addr d. Clear the terminal screen.

ACTIVITY 12-4

Configuring a DNS Client Service

Before You Begin:

You logged in to the GUI as root and the terminal window is displayed.

Scenario:

You obtained a domain name, ourglobalcompany.com, for OGC Systems. You want the DNS server to resolve the IP addresses 192.168.0.2 and 192.168.0.3 to the hostnames srvA.ourglobalcompany.com and srvB.ourglobalcompany.com. You want to configure the client to use the DNS server service.

What You Do	How You Do It
1. Add the DNS name server data to the /etc/resolv.conf file.	<div>a. To open the /etc/resolv.conf file in the vi editor, type vi /etc/resolv.conf</div> <div>b. To specify the IP address of the DNS server, enter nameserver 192.168.0.2</div> <div>c. Switch to command mode.</div> <div>d. Save and close the file.</div>
2. Check whether the DNS service resolves hostnames and IP addresses.	<div>a. To resolve the IP address of srvA, enter host srvA.ourglobalcompany.com</div> <div>b. Observe that the IP address of srvA is displayed.</div> <div>c. To resolve the hostname of the IP address 192.168.0.3, enter host 192.168.0.3</div> <div>d. Clear the terminal screen.</div>

TOPIC D

Manage Remote Network Systems

Previously, you configured network services to allow a system to access network resources. In situations such as adding new systems to a network, you will directly communicate with the system and modify data on the system to connect your computer to the other system. In this topic, you will explore SSH and VNC and examine their functions to communicate with remote systems.

As a system administrator, you will address the needs of users who are scattered across different locations. There may be some meetings or conferences that require you to connect to the server remotely. Your capability as a system administrator will increase if you know how to connect to remote systems. You can access data remotely and troubleshoot all systems from one location.

PKC

Definition:

Public Key Cryptography (PKC) is an encryption method that uses a public and private key pair. Data is encrypted using the public key and then transmitted through the network. When the data reaches its destination, it is decrypted using the private key.

Example:

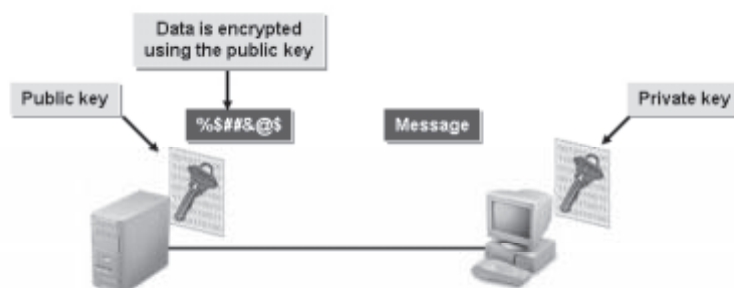


Figure 12-26: Encrypted data that uses both the keys.

The SSH

Definition:

Secure Shell (SSH) is a network protocol that securely controls the flow of data among computers on a network. SSH architecture contains the transport layer, the user authentication layer, and the connection layer. The client places a request that is authenticated by the user authentication layer. This layer transfers the request, which is authenticated by the transport layer, to the server through the connection layer. By making use of public-key cryptography to encrypt data, this architecture makes SSH flexible and secure. Many versions of SSH, such as SSH1 and SSH2, are available.

Example:

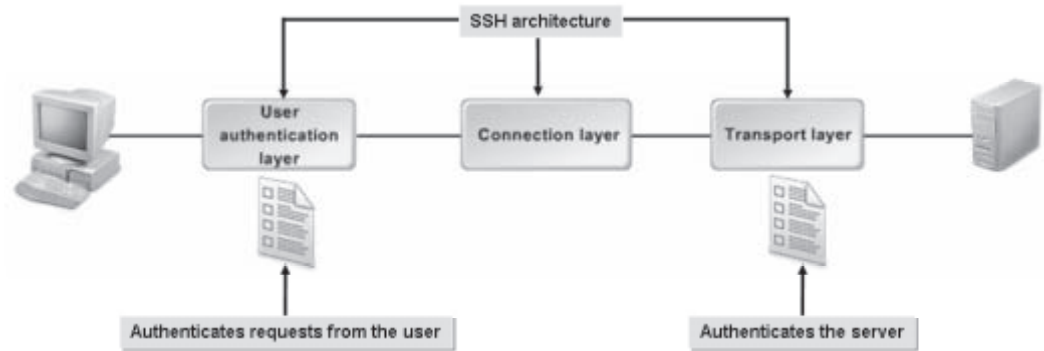


Figure 12-27: SSH controlling secure communication on a network.

OpenSSH

OpenSSH is a free version of the SSH protocol that is included with most Linux distributions. Data to be transmitted passes through a secure tunnel that is formed between two systems. Telnet transmits data, which includes passwords, that can be easily intercepted by any system on the network. OpenSSH provides a strong client-server authentication method for data transmitted by Telnet and similar applications.

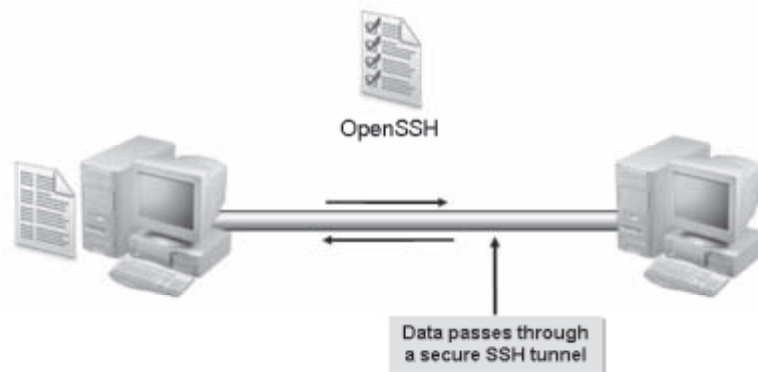


Figure 12-28: Data transfer using the OpenSSH tunnel.

The ssh-keygen Command

The *ssh-keygen* command generates, manages, and converts authentication keys. The following table lists some options of the *ssh-keygen* command.

Use This ssh-keygen Command Option	If You Need To
<code>-b {bits}</code>	Specify the number of bits to be created in the key.
<code>-c</code>	Change the comment in the public and private key files.
<code>-f {file name}</code>	Specify the file name of the key file.
<code>-l</code>	Show the fingerprint of the specified public key file.

Use This ssh-keygen Command Option	If You Need To
<code>-p</code>	Change the passphrase of a private key file instead of creating a new private key.

Public and Private Keys

Both private keys and public keys are involved in an authentication process. Each key is a collection of alphanumeric and special characters that uniquely identify each system. A private key is involved in public key authentication that is retained on the local system. A public key is involved in public key authentication that is made known to remote systems. The private key is retained on the local system. The public key is made known to remote systems. The private key is never transmitted to the destination server. A meaningful message will result only when the destination's private key is combined with the public key of the original server. While logging in to a remote system, the private and public keys are combined by the remote server for verification. The keys need to match if a user has to log in to the system and transfer files. Authenticity is established by the remote server, which then grants the necessary permissions.

Key Files

The key pairs that you create using SSH are stored in different files depending on the algorithm you use.

File Created	Algorithm
<code>id_dsa</code> and <code>id_dsa.pub</code>	DSA
<code>id_rsa</code> and <code>id_rsa.pub</code>	RSA with SSH protocol version 2
<code>identity</code> and <code>identity.pub</code>	RSA with SSH protocol version 1

OpenSSH on Debian

When you install openssh on a Debian system, two pairs (DSA and RSA authentications) of public and private keys are created in the `/etc/ssh` directory. The two pairs created are: `/etc/ssh/ssh_host_rsa_key` and `/etc/ssh/ssh_host_rsa_key.pub` and `/etc/ssh/ssh_host_dsa_key` and `/etc/ssh/ssh_host_dsa_key.pub`.

The `/etc/ssh/sshd_config` File

The `/etc/ssh/sshd_config` file is the SSH server configuration file. Most lines in this configuration file are commented, indicating the default settings that have been applied. You can remove the comment and change the default settings. A few SSH server configuration file options are listed in the following table.

Use This sshd Option	If You Need To
<code>X11Forwarding yes</code>	Run or stop running a program on one system and display the X window output on another system.

Use This sshd Option	If You Need To
<code>X11Forwarding no</code>	Stop running a program on one system and display the X window output on another system.
<code>PermitRootLogin</code>	Allow the root user to login via SSH.
<code>MaxStartups {number}</code>	Specify the maximum number of connections that can be made to a host.
<code>LoginGraceTime {time in seconds}</code>	Drop connections if the connection is not established within the login grace time.
<code>AuthorizedKeysFile {file name}</code>	Specify the location of the file that contains the authentication keys.
<code>PermitEmptyPasswords yes/no</code>	Specify whether a null password is allowed or denied.

The ssh-agent Program

Definition:

The *ssh-agent* program is a program that holds private keys for public key authentication. This program starts with an X-session or login session, and acts as a parent program, while all other programs or windows are its clients. The *ssh-agent* does not send a private key through channels; instead, the task that requires a private key is performed by the agent and the result is returned to the client. Initially, the agent does not have a private key. Keys are added using the *ssh-add* utility.

Example:



Figure 12-29: Role of *ssh-agent*.

Server Keys

When you install an SSH server, public host and server keys are automatically created for authentication purposes. The server keys are not stored anywhere in the disk; they are automatically regenerated every hour to ensure security.

The known_hosts File

When you connect to a remote host, the host sends you public host and server keys for authentication. Your system looks up the `~/.ssh/known_hosts` file to locate an entry for the host's keys, and if an entry is found, you will be allowed to access the host. Otherwise, a message is displayed, stating that the authenticity of the remote host is not yet established. You need to type "yes" to trust the remote host and connect to it. Whenever a SSH connection is made to a remote terminal, the public key of that system or host is added to the `~/.ssh/known_hosts` file.



The `~/.ssh/known_hosts` file was known as the `/etc/ssh_known_hosts` file in older versions of Linux.

The ~/.ssh/authorized_keys File

The public and private keys of the ssh client must be added to the ~/.ssh/authorized_keys file on the remote server.

SSH Protocol Versions

By default, both SSH protocol versions 1 and 2 are compatible with OpenSSH. Although using SSH 2 offers enhanced security benefits, you can use SSH 1 based on the client. To change the configuration, you can modify the `Protocol` option in the `sshd_config` file.

You can also specify OpenSSH to use SSH 2 by default and fall back on SSH 1, whenever needed, by modifying the `Protocol` option as `Protocol 2,1`

Multiple SSH Connections

If your network or firewall settings change while you are connected to the SSH server, you may lose the connection. To prevent such loss of connection, SSH allows multiple simultaneous connections from multiple hosts.

You can use the `MaxStartups` option to specify the maximum number of connections that can be made to a host. However, additional connections will be dropped only until the login grace time expires. The login grace time is specified using the `LoginGraceTime` option.

The SCP Command

SCP stands for secure copy. The `scp` command enables you to transfer secure copies of files over an encrypted remote network connection. The command uses SSH to provide security for data transfer and authentication, using passwords and passphrases.

Using the `scp` command, you can copy files from a remote system to your local host and vice versa. Furthermore, you can also transfer files between two remote systems, without involving your local system.

.rhosts and .shosts

Using `.rhosts` or `.shosts`, SSH allows users to log into another remote host with just a user name. A password or passphrase is not required for authentication. If the remote machine consists of the `.rhosts` or the `.shosts` files in the home directory, users are allowed to log in and access the machine. However, this method is a threat to the security because if users are allowed to access a remote machine without authentication, users can further access other machines that trust the first remote machine.

The sftp Command

The `sftp` command is used to create a secure FTP tunnel through SSH. Thus, it provides the functionality of FTP with the security of SSH. Secure FTP is compatible with all normal FTP commands in interactive mode.

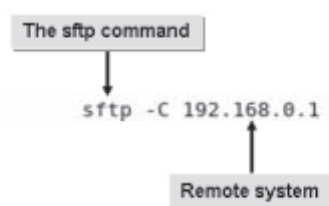


Figure 12-30: Connecting to a remote system using `sftp`.

Syntax

The syntax of the `sftp` command is `sftp {hostname}` or `sftp {user}@{hostname}`. The command can also be used with the `-C` flag to allow file compression.

Tunneling

Tunneling is a layered protocol model in which one protocol is layered over another. The inner protocol, called the payload protocol, is encapsulated within another protocol, which is called the delivery protocol. This provides security and flexibility to the connection. Some of the tunneling protocols are GRE, GTP, and MPLS.

An SSH tunnel is created when an SSH protocol connection is made. SSH tunneling enables users to access websites and bypass firewalls by setting up *proxy servers*. A protocol that is blocked by a firewall is encapsulated within a different protocol that is not blocked by the firewall, thus establishing the connection.

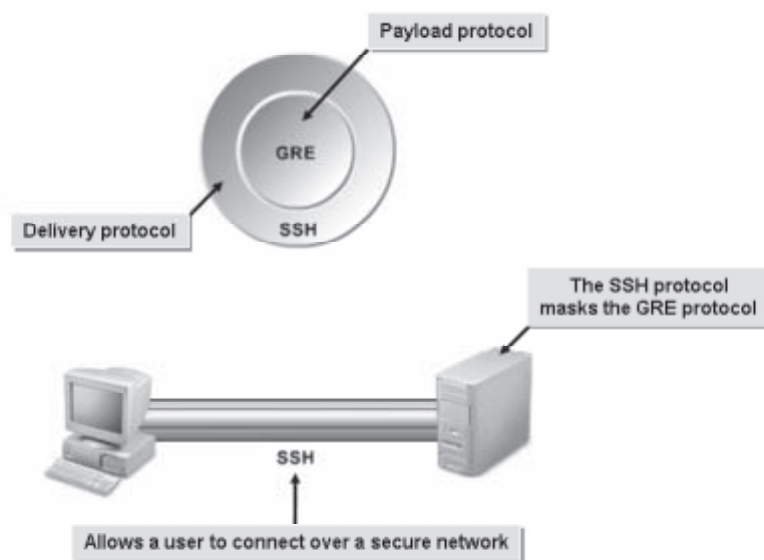


Figure 12-31: The tunneling protocol and its architecture.

X Forwarding

Definition:

X forwarding is a mechanism by which programs are run on one machine and the X window output is displayed on another machine. X forwarding can be enabled or disabled by setting the `X11Forwarding` option to `yes` or `no` in the `/etc/ssh/sshd_config` file. This allows X11 tunnelling over an SSH connection.

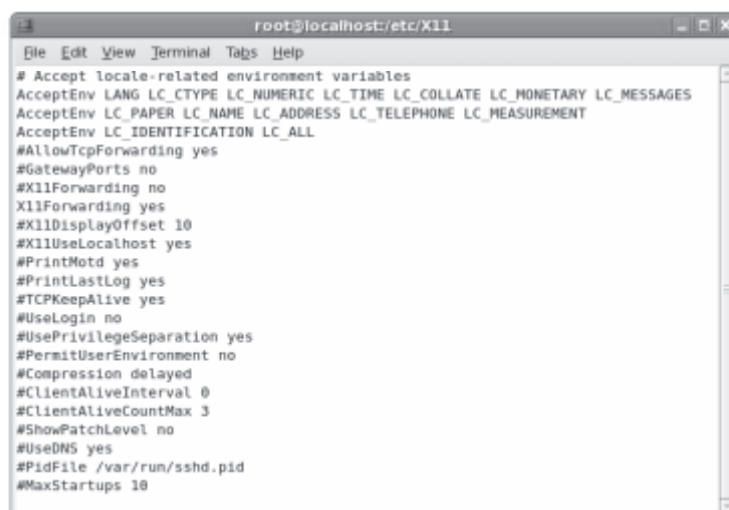
Example:

Figure 12-32: The X11 forwarding option enabled in the configuration file.

Port Forwarding

SSH secures the TCP/IP protocol using port forwarding. SSH can map a local port of the client to a remote port on the server. The following command is used to create a TCP/IP port forwarding channel:

```
ssh -L local-port:{remote-hostname}:{remote-port}
{username}@{hostname}
```

Port forwarding is also used to transfer information securely through network firewalls.

VNC**Definition:**

Virtual Network Computing (VNC) is a platform-independent system through which a user can control a remote system. The virtual network is made up of the VNC client, the VNC server, and the VNC protocol. The client views the output that is displayed by the server through the VNC protocol. The user can run multiple VNC sessions at any given time. However, the display for each VNC client may differ from the display of the VNC server.

Example:

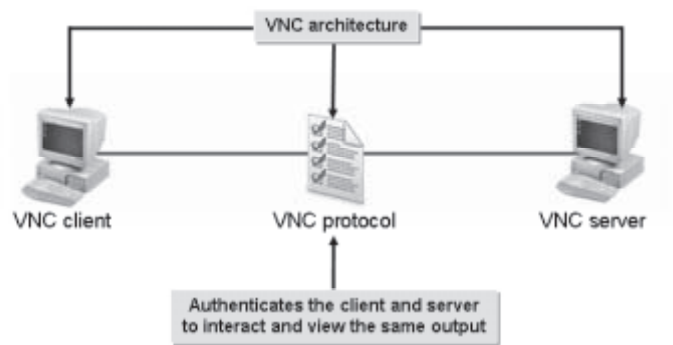


Figure 12-33: The VNC protocol enables the client to view the output displayed by the VNC server.

The vncserver Command

The `vncserver` command is used to start a system with VNC. The `$HOME/.vnc/xstartup` file allows a user to control applications running on a remote system. You can specify the display number that the VNC server will use when it is started.

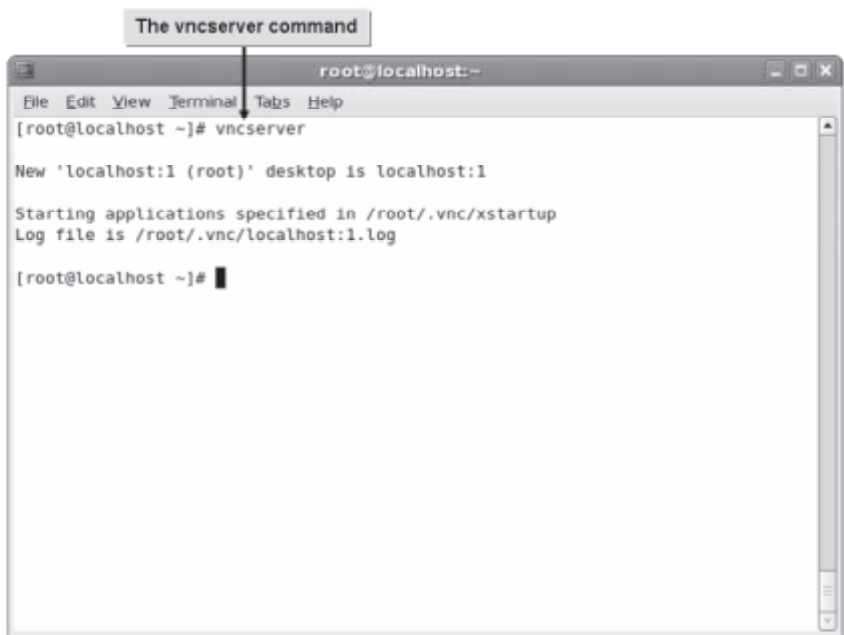


Figure 12-34: VNC enabled on a Linux system.

The `vncserver` command has various options.

Option	Enables You To
<code>-name {desktop name}</code>	Specify the desktop name.
<code>-geometry {resolution}</code>	Specify the screen resolution of the remote desktop.
<code>-depth {depth}</code>	Specify the pixel depth of the desktop. The accepted values are 8, 15, and 24.

Option	Enables You To
<code>-pixelformat {format}</code>	Specify the pixel format such as RGB and BGR.

Syntax

The syntax of the `vncserver` command is `vncserver {:display number} {options}`.

The vncviewer Command

The `vncviewer` command is used to view the VNC client. Various options are available for specifying `vncviewer` parameters.

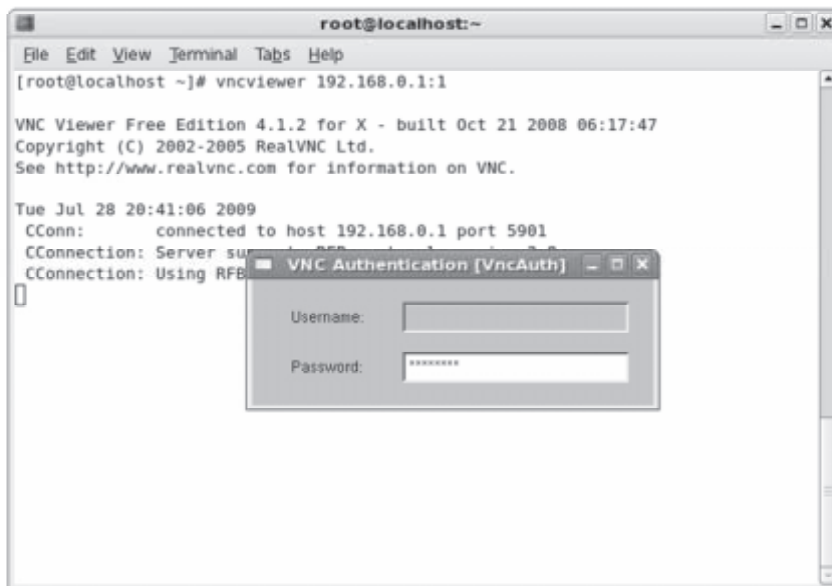


Figure 12-35: The `vncviewer` command is used to connect to a VNC server.

The `vncviewer` command has various options.

Option	Enables You To
<code>-display {Xdisplay}</code>	Specify the X display.
<code>-listen [port]</code>	Search for reverse connections from the VNC server.
<code>-Shared</code>	Keep multiple VNC connections open.
<code>-FullScreen</code>	Start the VNC client in full-screen mode.
<code>-via {gateway}</code>	Create a tunnel to a gateway system and then connects the client to the host.

The rdesktop Utility

`rdesktop` is an open source utility, released under GPL. It enables a client system running Linux to log in to a system running Microsoft Windows on a network. It supports Microsoft's Remote Desktop Protocol (RDP). The `rdesktop` command can be used to log in to a remote Windows system.

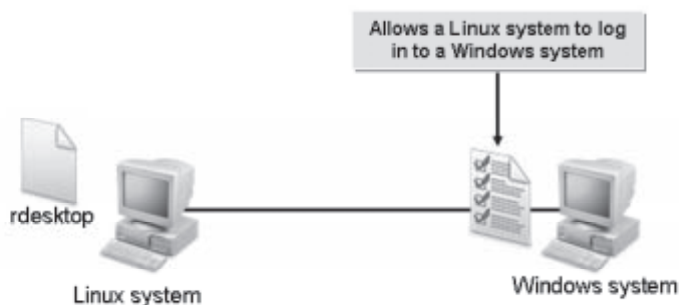


Figure 12-36: A Linux system logging in to a Windows system with the help of *rdesktop*.

Syntax

The syntax of the `rdesktop` command is `rdesktop [options] server[:port]`.

The rdesktop Command Options

Some frequently used `rdesktop` command options are listed in the following table.

Option	Used To
<code>-u {user name}</code>	Specify the user name for authentication on the server.
<code>-d {domain name}</code>	Specify the domain name for authentication.
<code>-s {application name}</code>	Start a specific application instead of Explorer.
<code>-c {directory}</code>	Specify the initial working directory for the user.
<code>-p {password}</code>	Specify a password for authentication.

RDP

RDP is a multi-channel protocol that allows users running various other operating systems to connect to a system running Microsoft Windows and vice versa, on a network.

The SNMP

The *Simple Network Management Protocol (SNMP)* enables you to remotely monitor and configure network components such as bridges, routers, network cards, and switches.

SNMP management requires two primary elements: a network manager and an SNMP agent.

Element	Description
Network manager	The software running on a workstation through which the network administrator monitors and controls the different hardware and software systems that comprise a network.
SNMP agent	A piece of software running on network equipment that implements the SNMP. The SNMP defines exactly how a network manager communicates with an SNMP agent.

RMON

Remote Monitoring (RMON) is a network management protocol that allows network information to be gathered at a single workstation. For RMON to work, network devices, such as hubs and switches, must support it.

How to Manage Remote Network Systems

Procedure Reference: Communicate Using Secure Shell

To communicate using secure shell:

1. Log in as a user.
2. Connect securely to another computer.
 - a. To connect to the remote host, enter `ssh {user name}@{hostname} / {IP of the destination}`.
 - b. If prompted, add the host as a trusted host.
 - c. To log in to the system, enter the password.
3. Execute commands securely in another computer.
 - a. To connect to the remote host, enter `ssh {user name}@{hostname} / {IP of the destination}`.
 - b. If prompted, add the host as a trusted host.
 - c. To log in to the system, enter the password.
 - d. To execute the required action, enter the command.
4. Create a tunnel using SSH.
 - a. To create a tunnel using SSH, enter `ssh -L {port number}:{remote server IP} / {FQDN}:{port number} {user name}@{remote server IP} / {FQDN}`.
 - b. If prompted, add the host as a trusted host.
 - c. To log in to the system, enter the password.
5. Authenticate the tunnel with SSH keys.
 - a. To generate a key, enter `ssh-keygen -d`.
 - b. To generate the keys **id_dsa** and **id_dsa.pub** in **/root/.ssh**, press **Enter** three times.
 - c. Log in as root in the second system with which you want to establish an SSH connection.

- d. Enter `ssh-keygen -d`.
- e. To generate the keys `id_dsa` and `id_dsa.pub` in `/root/.ssh`, press **Enter** three times.
- f. To copy the public key from the second system to the first system, enter `scp /root/.ssh/id_dsa.pub {user name}@{remote server IP} | {FQDN of the first system}:/root/.ssh/authorized_keys`.
- g. If prompted, add the host as a trusted host.
- h. To log in to the system, enter the password.
- i. To copy the public key from the first system to the second system, enter `scp /root/.ssh/id_dsa.pub {user name}@{remote server IP} | {FQDN of the first system}:/root/.ssh/authorized_keys`.
- j. If prompted, add the host as a trusted host.
- k. To log in to the system, enter the password.

Procedure Reference: Configure ssh-agent

To configure ssh-agent:

1. Open the `/etc/skel/.bash_profile` file.
2. Add a statement to provide the same ssh-agent whenever any user logs in.
`eval 'ssh-agent'`
3. Save and close the file.
4. Open the `/etc/skel/.bash_logout` file.
5. Add a statement to kill the ssh-agent when the user logs out.
`ssh-agent -k`
6. Save and close the file.

Procedure Reference: Transfer Files Securely to Another Computer

To transfer files securely to another computer:

1. Log in as a user in the CLI.
2. To transfer files using the `scp` utility, enter `scp {options} {source file or folder name} {user name}@{hostname} | {IP of the destination}:/ {destination file} or {folder name}`.
3. If prompted, add the host as a trusted host.
4. To transfer the file, enter the password.

Procedure Reference: Run the VNC Server

To run the VNC server:

1. Log in as root in the GUI.
2. On the terminal, enter `vncserver` to start the VNC server.
3. Enter the VNC server password, which will be used by clients when connecting to this server.

4. Confirm the password.
5. Write down the `{server name}:{screen number}` that is displayed.

Procedure Reference: Connect to the VNC Server Using the VNC Viewer

To connect to the VNC server using the VNC viewer:

1. Log in as root in the GUI of the client system.
2. To view the VNC server, on the terminal, enter `vncviewer {server name}:{screen number}`.
3. To connect to the VNC server, in the VNC Authentication window, in the **Password** text box, enter the password of the server.

ACTIVITY 12-5

Communicating Using the Secure Shell

Before You Begin:

1. On `srvA`, you have logged in as root in the CLI.
2. The first terminal is displayed.
3. At the command line, copy the `meeting_report` file from the `/085099Data/Configuring_Network` directory to the root directory of `srvA`.
4. To generate a key, enter `ssh-keygen -d`.
5. To generate the keys `id_dsa` and `id_dsa.pub` in `/root/.ssh`, press **Enter** three times.
6. Clear the terminal screen.

Scenario:

A lecture is scheduled to take place at your office. As a system administrator, you have been asked by users to establish a secure connection between the system in the lecture hall and their systems, so that they can access the `meeting_report` file on their systems remotely. You decide to configure the SSH to establish the connection and secure it using authentication keys.

LESSON 12

What You Do

How You Do It

1. Connect to another computer on the network.

- a. To connect to the server, at the command line, enter **ssh root@192.168.0.2**

- b. To continue, enter **yes**



If you are prompted to continue connecting, enter **yes**.

- c. If prompted, at the **root@192.168.0.2's password** prompt, enter **p@ssw0rd**

- d. Verify that the last login time is displayed.

- e. To view the contents of the **meeting_report** file, enter **cat meeting_report**

- f. Enter **logout**

2. Create a tunnel using SSH.

- a. To create a tunnel using the SSH, on srvB, enter **ssh -L 3128:192.168.0.2:3128 root@192.168.0.2**


- b. If prompted, to continue connecting, enter **yes**

- c. If prompted, at the **root@192.168.0.2's password** prompt, enter **p@ssw0rd**


- d. Verify that the last login time is displayed.

- e. Enter **logout**

3. Authenticate the tunnel with SSH keys.
 - a. To generate a key, enter **ssh-keygen -d**
 - b. Generate the keys **id_dsa** and **id_dsa.pub** in **/root/.ssh**.

 If prompted, to overwrite the file, enter **y**.
 - c. To copy the public keys to the server, enter **scp /root/.ssh/id_dsa.pub root@192.168.0.2:/root/.ssh/authorized_keys**
 - d. If prompted, at the **root@192.168.0.2's password** prompt, enter **p@ssw0rd**
 - e. Observe that the file is copied to the server.

 4. Copy the keys from the server to the client.
 - a. To connect to **srvA**, enter **ssh root@192.168.0.2**

 If you are prompted to continue connecting, enter **yes**.
 - b. If prompted, at the **root@192.168.0.2's password** prompt, enter **p@ssw0rd**
 - c. To copy the public keys to the client, enter **scp /root/.ssh/id_dsa.pub root@192.168.0.X:/root/.ssh/authorized_keys**
 - d. At the **Enter passphrase for key** prompt, press **Enter**.
 - e. If prompted, at the **root@192.168.0.X's password** prompt, enter **p@ssw0rd**
 - f. If necessary, to continue, at the prompt, enter **yes**
 - g. Observe that the file is copied to the client.
 - h. To log out of the server, enter **logout**
-

ACTIVITY 12-6

Implementing VNC

Before You Begin:

To be done on srvA:

1. You have logged in as root in the CLI.
2. Switch to the GUI.
3. Log in as root.
4. Display the terminal window.
5. Ensure that the packages `vnc-4.1.2-9.el5.i386.rpm` and `vnc-server-4.1.2-9.el5.i386.rpm` are installed before commencing with this activity. Otherwise, you can install the packages using the `yum localinstall /rhelsource/Server/vnc*` command.
6. To start the VNC server, in the terminal window, enter `vncserver`.
7. Enter the VNC server password that is used by the clients when connecting to this server.
8. Confirm the password.
9. Make a note of the server name and the screen number that is displayed.



Instead of the server name, the IP address of the server can also be used.

10. To create the employee directory, enter `mkdir /employee`.
11. To clear the terminal window, enter `clear`.

Before You Begin:

To be done on srvB:

1. You have logged in as root in the CLI.
2. Switch to the GUI.
3. If necessary, install the VNC viewer package.

Scenario:

As the system administrator, you want to maintain a list of users and their IP addresses to track network resources. You find that system details of the users have not been updated on the server.

What You Do

How You Do It

1. Connect to the VNC server using `vncviewer`.

- a. To view the VNC server, enter **`vncviewer 192.168.0.2:X`**
- b. In the VNC Authentication window, in the **Password** text box, enter **`p@ssw0rd`**
- c. Position the mouse pointer on the terminal.



In the place of X, students should type their respective screen numbers provided by the instructor.

2. Create the employee file in the /employee directory.

- a. To navigate to the employee directory, enter **`cd /employee`**
- b. To create the employee file, enter **`vi employee192.168.0.X`**



In the place of X in employee192.168.0.X, students should enter their respective system numbers.

- c. To switch to insert mode, press **I**.
- d. Enter **`Name=XXXXX`**



In the place of XXXXX, students should enter their name.


- e. Enter **`Employee IP=192.168.0.X`**



In the place of X, students should enter their respective system numbers.

- f. To exit command mode, press **Esc**.
- g. Save and close the file.
- h. To exit the VNC server, click the **Close** button.
- i. To close the terminal window, enter **`exit`**

LESSON 12

3. Verify that the file was successfully created.
 - a. Switch to `srvA`.
 - b. To change to the employee directory, in the terminal window, enter `cd /employee`
 - c. To view the contents of the file, enter `cat employee192.168.0.X`
 In the place of X, students should enter their respective system numbers.
 - d. Observe that the contents of the file are displayed, which indicates that the file was successfully created.
 - e. To clear the terminal window, enter `clear`
-

Lesson 12 Follow-up

In this lesson, you configured and managed various network services and remote network systems. You will now be able to disseminate information, administer systems remotely, enable communication through mail or chat systems, facilitate technology sharing, manage software licenses, and control unauthorized access.

1. What are the advantages of managing IP addresses centrally on a network?
2. Discuss the points that must be considered before you enable DNS on a network.

LESSON 13

Configuring Basic Internet Services

Lesson Time

2 hour(s)

In this lesson, you will configure basic Internet services.

You will:

- Configure email services.
- Control Internet services.

Introduction

In the last lesson, you configured network services. Now, you want to implement a business-oriented service that allows you to share resources and communicate across various platforms on a network. In this lesson, you will configure basic Internet services.

The Internet offers various services such as email, file sharing and downloading, and web browsing. Employees of an organization will often need to access the Internet and communicate with clients across various platforms. As a system administrator, you want to implement a simplified service that provides interoperability among applications and involves cost-effective communication. Internet services facilitate the ability to share and transfer resources across various networks securely.

This lesson covers all or part of the following CompTIA Linux+ Powered by LPI certification objectives:

- Topic A:
 - Objective 108.3, Objective 109.1
- Topic B:
 - Objective 109.1, Objective 110.2
- Topic D:
 - Objective 110.2

TOPIC A

Configure Email Services

In the previous lesson, you configured basic network services. Now, you need to share information through the Internet because this is the most simplified and standardized way of communication and provides client and server email services by defining the email process. In this topic, you will configure email services.

It wasn't long ago that organizations conducted business communications using only the internal mail room and the postal service. Today, however, we communicate electronically with email and instant messaging. Understanding how mail clients operate is critical to implement an email service.

Mail Protocols

Definition:

A mail protocol is a set of rules that enable distribution of email messages from a mail server. Using a mail protocol, an email message may be stored on a server or transmitted to a client's computer when read. Mail protocols enable users to create and manage folders on a server, search for messages, or delete messages. POP, IMAP, and SMTP are the most frequently used mail protocols.

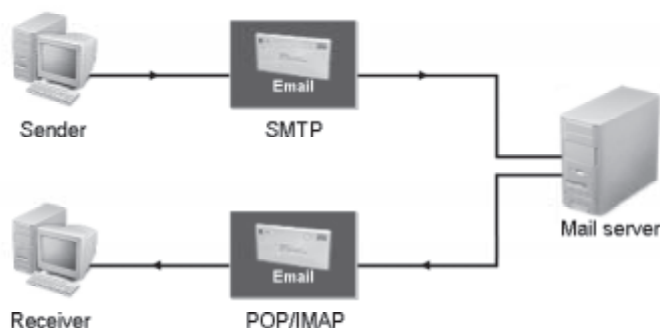
Example:

Figure 13-1: Email messages are distributed using the POP, IMAP, and SMTP protocols.

The SMTP

The *Simple Mail Transfer Protocol (SMTP)* is a protocol that defines a set of rules to enable interaction between a program sending an email message to a server and a program receiving an email message from a client. The Mail Transfer Agent (MTA) or the Mail User Agent (MUA) acts as an SMTP client. The SMTP server always listens to port 25 for client responses. SMTP uses TCP for transmitting messages and IP for routing purposes. It contains a number of status codes that are used to set specific conditions for communication between the server and the client. It also contains a set of commands that are used for communication between the server and the client.

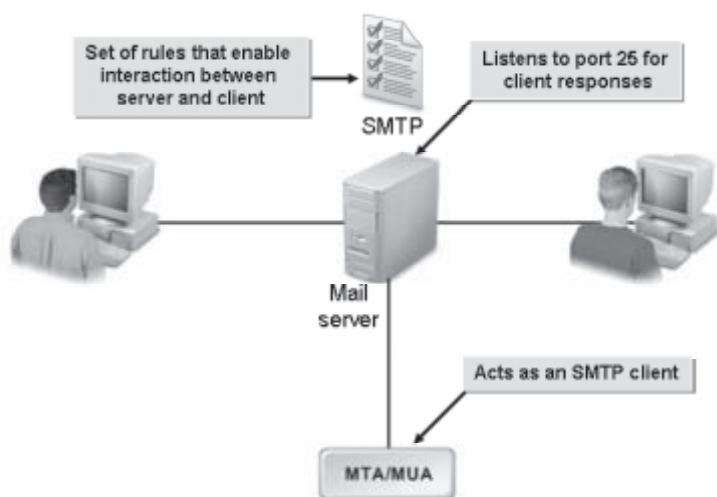


Figure 13-2: Communication between clients using SMTP.

In addition to text messages, graphics and attachments can also be transferred through email using Extended SMTP (ESMTP). The Extended HELLO (EHLO) command is used by ESMTP clients to communicate with the server, and the server responds with one of the three status codes: success, failure, or error.

Mail Spooling

Spooling is a method of handling delays in delivering email messages. If there is an email delivery delay, SMTP at the originating computer spools the message. If there is no delay, SMTP at the originating computer sends the email message to the destination computer using the TCP connection. SMTP on the destination computer receives the email message and puts it in the user's mailbox. The same process occurs in reverse when a user at the destination computer sends a reply to a user at the originating computer.

POP3

Post Office Protocol version 3 (POP3) is used to retrieve email messages over the TCP connection on port 110. The POP client connects to the server and retrieves all messages. It then stores them on the client PC as new messages, deletes them from the server, and disconnects from the server. It supports MIME formatted email messages. In general, POP3 supports the transmission of messages and passwords in clear text format. It also provides authentication by encrypting the messages using the SSL protocol over TCP on port 995.

IMAP

The *Internet Message Access Protocol (IMAP)* is used to retrieve email messages over the TCP connection on port 143. The client retrieves all messages from the server, which retains them until they are deleted by the user. Although the protocol transmits messages and passwords in clear text format, it supports SSL encryption of messages over TCP on port 993. In addition, it supports MIME formatted email messages.

Mail Queues

Definition:

A *mail queue* is a waiting area for email messages that need to be processed by a computer. Mail queues are organized in such a way that the first item added to a queue is also the first item that is sent out of the queue.

Example:

```

root@localhost:~
File Edit View Terminal Tabs Help

[root@localhost ~]# mailq
-Queue ID- --Size-- ----Arrival Time---- -Sender/Recipient-----
0E679330573    2633 Thu Jul 30 20:05:39 MAILER-DAEMON
      (connect to srvB.ourglobalcompany.com[192.168.0.2]: Connection refused)
      root@srvB.ourglobalcompany.com

C14AC330566    2584 Thu Jul 30 19:52:03 MAILER-DAEMON
      (connect to srvB.ourglobalcompany.com[192.168.0.2]: Connection refused)
      root@srvB.ourglobalcompany.com

B9F20330568    2567 Thu Jul 30 19:52:03 MAILER-DAEMON
      (connect to srvB.ourglobalcompany.com[192.168.0.2]: Connection refused)
      root@srvB.ourglobalcompany.com

-- 8 Kbytes in 3 Requests.
[root@localhost ~]#
  
```

Figure 13-3: Email messages are arranged in a queue.

The MTA

Definition:

The *Mail Transfer Agent (MTA)* is a program on the Internet for sending email messages using SMTP. They use SMTP to indicate the success or failure in the delivery of messages and to form separate queues for failed messages. MTAs often use the Local Mail Transport Protocol (LMTP), a derivative of SMTP, when mail queues are not allowed to be stored on the server end. MTAs allow clients to handle mail queues instead of the server and do not provide mailbox handling features.

Example:

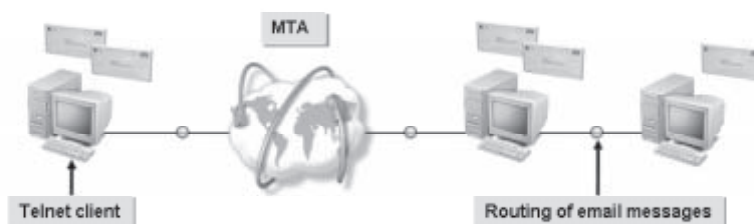


Figure 13-4: Routing of email messages through the MTA.

Types of MTAs

MTAs support features such as virtual hosting, automatic resending of messages in case of failed delivery, and spamassassin—a mail filter that is used to identify spam messages. Each MTA supports various features providing default access control on the server.

MTA	Description
Sendmail	A standard MTA that supports various Unix-based operating systems. It is designed to function in such a way that it runs as a single entity. It supports various MTAs and MDAs. It is an MTA that is still used from earlier days.
Postfix	A fast and secure MTA that can be administered easily. It is similar to Sendmail but varies in its internal functionality. Unlike Sendmail, Postfix supports a modular functionality. It is a free, open MTA and can be used as an alternative for Sendmail.
Exim	A flexible and a freely available MTA. Unlike other MTAs, it has extensive features that allow the administrator to control the mail transfer through the system. The latest version has been developed into an ACL-based system, which provides more detailed and flexible controls. This helps in the integration of antivirus and anti-spam measures in the MTA.
Qmail	The first secure mail transfer agent that manages large mailing lists. It is made up of several modules, which can be replaced by any of the new modules that contain the same interface. It introduces the concept of wild cards, which allows users to publish multiple mail addresses for mailing lists.

Sendmail Configuration Files

When you install Sendmail, configuration files are created in the `/etc/mail` directory. The `sendmail.cf` file is the main configuration file for Sendmail. Because the configuration file is large, it is better to avoid editing the file directly. Instead, you can make changes to the `sendmail.mc` file and later update the `sendmail.cf` file using the `m4` utility.

Postfix Configuration Files

Postfix configuration files are created in the `/etc/postfix` directory. The `main.cf` and the `master.cf` are the two main Postfix configuration files. The `main.cf` file defines the configuration parameters and the `master.cf` file defines the daemon processes. Most of the configuration parameters are set to their default values. The `master.cf` file primarily defines the process of a client program connecting to a service and a daemon running when a service is requested.

Qmail Configuration Files

All Qmail configuration files, except the `.qmail` file, are stored in the `/var/qmail/control` directory. The `.qmail` file resides in the `~alias` directory of the user's home directory. The `.qmail` files are used to control the delivery of mail. They contain a list of delivery instructions represented by some special characters.

Exim Configuration Files

The configuration files of exim are created in the `/etc/exim` directory. The `exim.conf` file is the main configuration file for exim.

Sendmail Emulation Layer Commands

The `smrsh` program is a shell utility that restricts users from performing malicious actions and limits the programs that such users can execute. It acts as a replacement for `/bin/sh` in the program mailer definition for Sendmail and is installed in the `/usr/sbin/smrsh` directory. When the `smrsh` program is used along with Sendmail, Sendmail only executes the set of programs specified in the `smrsh` directory. The set of commands that the `smrsh` program allows Sendmail to execute are referred to as Sendmail emulation layer commands. Some of the interpreter programs prohibited from execution are `sh`, `csh`, `perl`, and `sed`.

The MUA

Definition:

The *Mail User Agent (MUA)* is a program used for reading and composing email messages. Also referred to as an email client application, the MUA acts as an interface between a user and an MTA and contains mailboxes for storing messages. MUAs can have either a graphical interface, such as Thunderbird and Evolution Mail, or a text-based interface such as `mutt`.

Example:



Figure 13-5: MUA acts as an interface between a user and MTA.

The MDA

Definition:

A *Mail Delivery Agent (MDA)* is a program that delivers incoming email messages to the intended recipient's mailbox. An MDA sends new mail messages using SMTP, and retrieves messages using POP3 or IMAP. It also distributes and sorts messages on a local machine so that an MUA can access them.

Example:

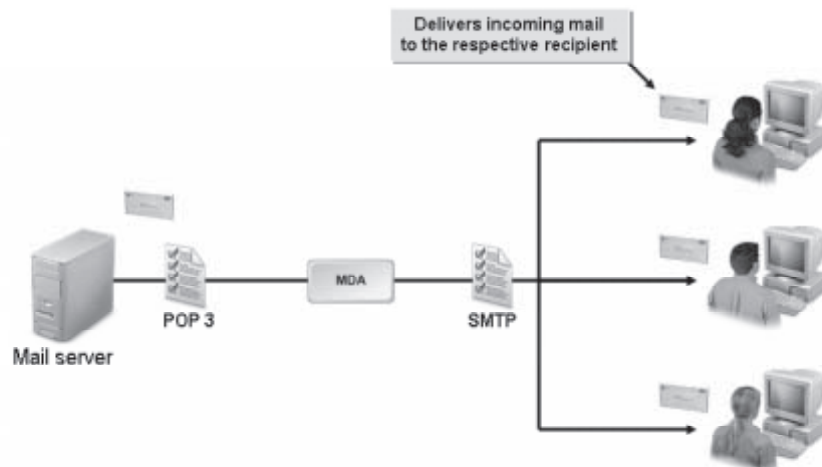


Figure 13-6: Email messages are delivered to clients using the MDA.

Mail Forwarding

Mail forwarding is a feature that automatically forwards email messages. It can also redirect mail to one or more addresses.

The Electronic Mailing Process

The electronic mailing process describes the sequence of steps involved in creating, transmitting, and storing messages. There are five stages involved in the electronic mailing process.

1. The sender composes the message to be sent. The sender's MUA formats the message in an email format and uses SMTP to send the message to the sender's MTA.
2. The sender's MTA checks for the destination address provided by SMTP. Based on the destination address, it sends a request to the DNS server to look for the specific domain name in the DNS server using UDP. The DNS server sends a response with an MX record that lists the mail exchange servers supported by the domain.
3. Based on the response from the DNS server, the sender's MTA sends the message to the recipient's MTA using SMTP.
4. The recipient's MTA again sends the message to the recipient's MDA, which delivers the email to a spool where all the recipient's messages are stored.
5. And, the recipient's MUA retrieves the message from the spool through a retrieval agent known as the *Mail Retrieval Agent (MRA)* using protocols such as POP3 and IMAP. The recipient then opens the received message.

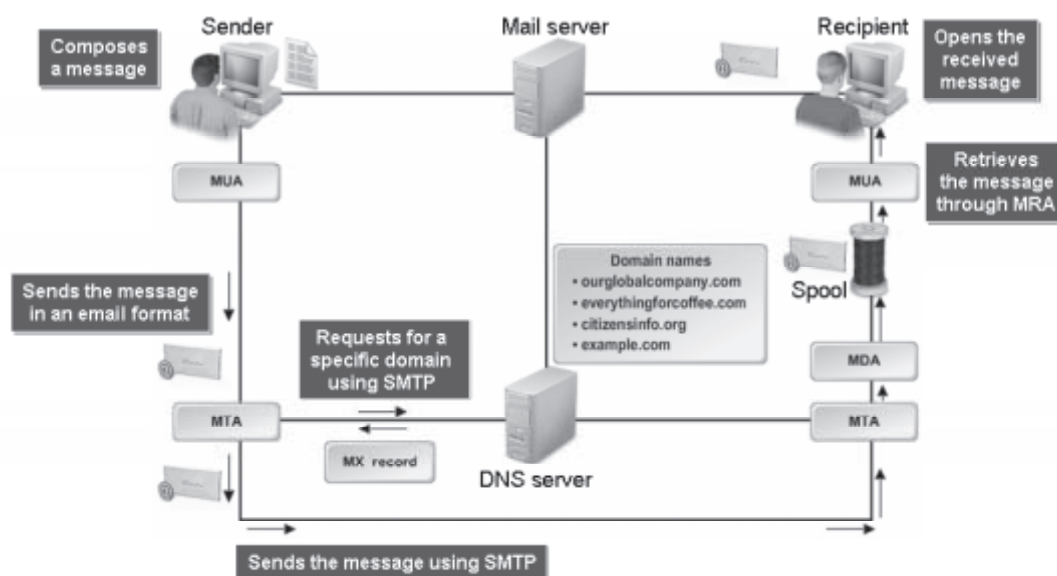


Figure 13-7: The process of sending an email message from one system to another.

How to Configure Email Services

Procedure Reference: Install Postfix

To install Postfix:

1. Log in as root.
2. Mount the Red Hat Enterprise Linux installation media containing postfix.
3. Navigate to the `/media/[name of the media]/Server` directory.
4. To install postfix, at the command line, enter `rpm -ivh postfix-{version}.{release}.i386.rpm`.
5. To verify that postfix has been installed, enter `rpm -qi postfix`.

Procedure Reference: Configure Postfix for Incoming Email Messages

To configure Postfix for incoming email messages:

1. Log in as root.
2. Set the Fully Qualified Domain Name.
 - a. Enter `hostname {Fully Qualified Domain Name}`.
 - b. Open the `/etc/sysconfig/network` file and ensure that the Fully Qualified Domain Name is updated.
3. Using the vi editor, open the `/etc/postfix/main.cf` file.
4. To receive mail messages from remote servers, set the system.
 - a. Locate the `"inet_interfaces = all"` directive and uncomment the line.
 - b. Locate the `"inet_interfaces = localhost"` directive and comment the line.

5. To specify a list of domains controlled by the postfix mail server, locate the “mydestination” directive and uncomment the line. `mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain, mail.$mydomain, www.$mydomain`
6. Save and close the file.
7. To start the postfix service, enter `service postfix start`.
8. To verify that the postfix server is listening to all interfaces, enter `netstat -plt | grep master`.
9. To enable the postfix service during system startup, enter `chkconfig postfix on`.

Procedure Reference: Configure Postfix for Outgoing Email Messages

To configure Postfix for outgoing email messages:

1. Log in as root.
2. Navigate to the `/etc/postfix` directory.
3. Using the vi editor, open the `main.cf` file.
4. Masquerade the domain for outgoing email messages.
 - a. Locate the “myorigin” directive and uncomment it.
 - b. To masquerade the root user, type `masquerade_exceptions = root`.
5. Save and close the file.
6. To restart the postfix service, enter `service postfix restart`.

Procedure Reference: Configure Email Aliases Using Sendmail or Exim

To set an email alias using Sendmail or Exim:

1. Using the vi editor, open the `/etc/aliases` file.
2. Add email aliases. An alias can be a local user name or a file name, a command, an include file, or an external address. `{user name}:{alias1}, [alias2, alias3,...]`
 - Add an alias for a user name that exists on the local system. `{user name}:{alias name for the user}`
 - Add an alias for an external email address to which you want the message to be forwarded. `{alias name}:{email address}`
 - Add an alias for a list of users to whom you want the mail to be forwarded. The list of users is specified in a separate file. `{user name}:include: {path to the file containing user names}/{file name}`
 - Add a file name to which you want to append the messages received by a user. `{user name}:{path to the file}/{file name}`
 - Or, add an alias to enable Sendmail process commands that receive messages from the standard input. `{user name}:<{command}`
3. Save and close the file.
4. To update the aliases database file, enter `newaliases`.

Procedure Reference: Configure Email Aliases Using Postfix

To configure email aliases using Postfix:

1. Using the vi editor, open the `/etc/postfix/main.cf` file.
2. Verify whether the `alias_maps` variable is defined with the location of the aliases file.

```
alias_maps = hash:/etc/aliases
```

3. Save and close the file.
4. Using the vi editor, open the `/etc/aliases` file.
5. Add an alias for a user name that exists on the local system.
`{user name}:{alias name for the user}.`
6. Save and close the file.
7. To update the aliases database file, enter `newaliases`.
8. To restart the postfix service, enter `service postfix restart`.

Procedure Reference: Configure Local Aliases

To configure local aliases:

1. Log in as root.
2. Using the vi editor, open the `/etc/postfix/main.cf` file.
3. Locate the `alias_maps` directive and verify whether the directive is defined with the location of the aliases file, in the format `alias_maps = hash:/etc/postfix/aliases`
4. Locate the `alias_database` directive and verify whether the directive is defined with the location of the aliases file, in the format `alias_database = hash:/etc/postfix/aliases`
5. Save and close the file.
6. Using the vi editor, open the `/etc/postfix/aliases` file.
7. Add email aliases.

```
{user name}:{alias1}, [alias2, alias3]
```

- Add an alias to a user name that exists on the local system.

```
{user name}:{alias name for the user}
```

- Add an alias to an external email address to which the mail is to be forwarded.

```
{user name}:email address
```

- Add an alias to a file that contains the list of users to whom the mail messages are to be forwarded.

```
{user name}:include:{path to the file containing user names}|{file names}
```

- Add an alias to the Sendmail command that receives messages from the standard input.

```
{user name}:{command}
```

8. Save and close the file.
9. To update the alias database file, enter `postalias /etc/postfix/alias`.
10. To restart the postfix service, enter `service postfix restart`.

Procedure Reference: Configure Virtual Aliases

To configure virtual aliases:

1. Log in as root.
2. Configure the prerequisite settings for virtual alias.
 - a. Using the vi editor, open the `/etc/postfix/main.cf` file.
 - b. Locate the `mydestination` directive and define the domains that will be controlled by the mail server. `mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain, mail.$mydomain, www.$mydomain, /etc/postfix/mydestination`
 - c. Save and close the file.
 - d. Using the vi editor, open the `/etc/postfix/mydestination` file.
 - e. To specify the list of domains that are controlled by the postfix, type *List of domains*. A sample `mydestination` file will be as given below.


```
ourglobalcompany.com
ourglobalcompany.org
ourglobalcompany.net
```
 - f. Save and close the file.
3. Using the vi editor, open the `/etc/postfix/main.cf` file.
4. Define the `virtual_alias_maps` variable below the `alias_maps` variable.


```
virtual_alias_maps = hash:/etc/postfix/virtual_maps
```
5. Save and close the file.
6. Using the vi editor, open the `/etc/postfix/virtual_maps` file.
7. Map email addresses to user names.


```
{user name@domain name} {user name}.
```
8. Map email messages destined to a domain to a specific user in another domain.


```
@{domain name} {user name@domain name}
```
9. Map email messages destined to a domain to another domain.


```
{user name}@{domain name1} {user name@domain name2}.
```
10. Save and close the file.
11. To rehash the virtual alias file, enter `postmap virtual_maps < virtual_maps`.
12. To restart the postfix service, enter `service postfix restart`.

Procedure Reference: Configure Outbound Address Rewriting

To configure outbound address rewriting:

1. Log in as root.

2. Navigate to the `/etc/postfix` directory.
3. Using the `vi` editor, open the `main.cf` file.
4. To enable outbound address rewriting, below the definition of the `alias_maps` directive, type `smtp_generic_maps = hash:/etc/postfix/generic_map`.
5. Save and close the file.
6. Using the `vi` editor, create a file, `generic_map`.
7. Type `{user name@domainname1} {user name@domainname1}`
8. Save and close the file.
9. To rehash the file, enter `postmap generic_map < generic_map`.
10. To restart the postfix service, enter `service postfix restart`.

Procedure Reference: Forward Incoming Mail Messages to a Different Address

To forward incoming mail messages to a different address:

1. Log in as user.
2. Enter `vi ~/.forward`.
3. Type the email address to which the incoming mail messages should be forwarded.
4. Save and close the file.
5. Verify that the messages have been forwarded to the address specified in the `~/.forward` file by sending an email to the user who has the forward file.
 - a. Enter `mail {user}`.
 - b. Specify a subject for the email and press **Enter**.
 - c. Specify content for the email. In the last line, type a period (`.`) and press **Enter**.
 - d. Specify the Carbon Copy recipients and press **Enter**.
 - e. Log out and log in as the user mentioned in the `~/.forward` file.
 - f. Enter `mail` to view the mailbox.
 - g. Enter the mail number to read the email.
 - h. If necessary, to delete the email, enter `D`.
 - i. To save and quit the mailbox, enter `Q`.

Procedure Reference: Manage a Mail Queue

To manage a mail queue:

1. Send an email message.
 - a. Log in as root in the CLI.
 - b. Enter `mail {user name}@{domain name}`.
 - c. Enter a subject for the message.
 - d. Enter content for the message and end the last line with a period.
 - e. Enter the Carbon Copy recipients.

2. Enter `mailq` to check whether the email message has been sent or is in queue.
3. If necessary, enter `rm -f /var/spool/mqueue/*` to remove the mail messages in the queue.



The `mailq` command is used to display the mail queue.

Procedure Reference: Configure Postfix Restrictions

To configure postfix restrictions:

1. Log in as root.
2. Using the vi editor, open the `/etc/postfix/main.cf` file.
3. To define restrictions for the sender, at the end of the file, enter
`smtpd_sender_restrictions = check_sender_access`
`hash:/etc/postfix/sender_access, [comma separated list`
`of zero or more mail sender restrictions].`
4. To define restrictions for the client, enter `smtpd_client_restrictions =`
`check_sender_access hash:/etc/postfix/client_access,`
`[comma separated list of zero or more mail client`
`restrictions].`
5. To define restrictions for the recipient, enter
`smtpd_recipient_restrictions = check_sender_access`
`hash:/etc/postfix/recipient_access, [comma separated`
`list of zero or more mail client restrictions].`
6. Save and close the file.
7. Navigate to the `/etc/postfix` directory.
8. Open the sender, recipient, or client access file.
9. Define the restrictions.
 - To allow relaying, type `{domain name} RELAY`.
 - To accept mail messages from the domain specified, type `{domain name} OK`.
 - To reject the mail messages sent from the domain specified, type `{domain name} REJECT`.
 - To reject the mail from the sender and display an arbitrary message, type `{domain name} ERROR:### message`.
 - To discard messages after accepting them, type `{domain name} DISCARD`.
10. Save and close the file.
11. To build the respective access database, enter `postmap {sender or`
`recipient or client access file} <postmap {sender or`
`recipient or client access file}`.
12. To restart the postfix service, enter `service postfix restart`.

ACTIVITY 13-1

Configuring Postfix

Before You Begin:

1. On *srvA*, switch to the GUI. Choose **System→Administration→Network**. In the **Network Configuration** dialog box, select the **DNS** tab.
2. In the **Hostname** text box, type *srvA.ourglobalcompany.com* and press **Tab**. Enter *192.168.0.2* as the primary DNS and the DNS search path.
3. Select the **Hosts** tab and click **New**. In the **Add / Edit Hosts entry** dialog box, in the **Address** text box, type *192.168.0.2* as the IP address. In the **Hostname** text box, enter *srvA.ourglobalcompany.com* as the hostname. In the **Aliases** text box, enter *srvA ourglobalcompany.com* as the aliases.
4. In the **Add / Edit Hosts entry** dialog box, click **OK**. Select the **Device** tab. Save the configuration and click **Activate** to restart the network service.
5. In the **system-config-network** message box, click **Yes**.
6. In the **system-config-network** message box, click **OK**.
7. On *srvA*, switch to the CLI. You have logged in as root in the CLI. The first terminal is displayed. To stop the sendmail service, at the command line, enter `service sendmail stop`. To disable the sendmail service during system startup, enter `chkconfig sendmail off`. Clear the terminal screen.
8. On *srvB*, switch to the GUI. Choose **System→Administration→Network**. In the **Network Configuration** dialog box, select the **DNS** tab. In the **Hostname** text box, type *srvB.ourglobalcompany.com* and press **Tab**. Enter *192.168.0.2* as the primary DNS and the DNS search path.
9. Select the **Hosts** tab and click **New**. In the **Add / Edit Hosts entry** dialog box, in the **Address** text box, type *192.168.0.3* as the IP address. In the **Hostname** text box, enter *srvB.ourglobalcompany.com* as the hostname. In the **Aliases** text box, enter *srvB* as the aliases. In the **Add / Edit Hosts entry** dialog box, click **OK**.
10. Select the **Devices** tab and click **Edit**. In the **Ethernet Device** dialog box, select the **Statically set IP addresses** option. Click in the **Address** text box, type *192.168.0.3* as the IP address, and press **Tab**. In the **Subnet mask** text box, type *255.255.255.0* and press **Tab**. In the **Default gateway address** text box, type *192.168.0.2*, and click **OK**.
11. Save the configuration and click **Activate** to restart the network service. To close the Network Configuration window, choose **File→Quit**. Switch to the CLI of *srvA*. Clear the terminal screen.
12. In the **system-config-network** message box, click **Yes**.
13. In the **system-config-network** message box, click **OK**.

Scenario:

Your company has already implemented a mail server using Sendmail for the domain *ourglobalcompany.com*. Now, due to organizational growth, the number of users accessing the mail server has increased, affecting the performance of the server. As the system administrator, you decide to migrate the mail server from Sendmail to Postfix.



In steps 2 and 7, change the IP address as *192.168.0.X* to match your DNS server address.

LESSON 13

What You Do

How You Do It

1. Install Postfix.

- a. On the system labeled srvA, type **yum localinstall /rhelsource/Server/postfix-2.3.3-2.1.el5_2.i386.rpm** and install the **postfix-2.3.3-2.1.el5_2.i386.rpm** package.
- b. To continue, enter **y**
- c. To set postfix as the default MTA, enter **alternatives --set mta /usr/sbin/sendmail.postfix**

2. Configure incoming mail on the server labeled srvA.

- a. Navigate to the /etc/postfix folder.
- b. Using the **vi** editor, open the main.cf file.
- c. Locate the line "inet_interfaces = all" and uncomment it.
- d. Locate the line "inet_interfaces = localhost" and comment it.
- e. To switch to command mode, press **Esc**.
- f. Locate the "#mydestination = \$myhostname" code.
- g. Uncomment the lines
#mydestination = \$myhostname,
localhost.\$mydomain, localhost,
\$mydomain, and #mail.\$mydomain,
www.\$mydomain, ftp.\$mydomain.

3. Configure email aliases on the server labeled srvA.
 - a. Locate the "alias_maps = hash:/etc/aliases" directive.
 - b. The cursor is placed after `alias_maps = hash:.` To change the alias file location to `/postfix/aliases`, move the cursor to end of `/etc/`. Enter **postfix/**
 - c. To switch to command mode, press **Esc**.
 - d. Locate the "alias_database = hash:/etc/aliases" directive.
 - e. The cursor is placed after `alias_database = hash:.` To change the alias file location to `/postfix/aliases`, move the cursor to the end of `/etc/`. Enter **postfix/**
 - f. To switch to command mode, press **Esc**.
 - g. Save and close the file.
 - h. Using the `vi` editor, open the aliases file.
 - i. Enter **hr: chris, pat,**
 - j. Type **root: jsmith**
 - k. To switch to command mode, press **Esc**.
 - l. Save and close the file.
 - m. To update the aliases database file, enter **postalias /etc/postfix/aliases**
 - n. Start the postfix service.
 - o. To run on booting the system, set the postfix service.
-

LESSON 13

4. Check the mail configuration.
 - a. Switch from the system labeled `srvA` to the system labeled `srvB`. Switch to the CLI.
 - b. On the system labeled `srvB`, enter `mail hr@ourglobalcompany.com`
 - c. At the **Subject** prompt, enter **Test mail - Postfix**
 - d. Enter **This is a test mail for postfix.**
 - e. Type a period (`.`) and press **Enter**.
 - f. At the **cc** prompt, press **Enter**.
 - g. Switch from the system labeled `srvB` to the system labeled `srvA`.
 - h. On the system labeled `srvA`, enter `mail -u chris`
 - i. Observe that the mail with the subject "Test mail - Postfix" is displayed.
 - j. Quit the mailbox.
 - k. View the mail messages in `pat`'s mailbox and quit the mailbox.
 - l. To clear the terminal screen, enter `clear`
-

5. Define email restrictions on srvA.

a. Using the `vi` editor, open the `main.cf` file.

b. To define sender restrictions, at the end of the file, enter

```
smtpd_sender_restrictions =
check_sender_access
hash:/etc/postfix/sender_access
```

c. To define recipient restrictions, at the end of the file, enter

```
smtpd_recipient_restrictions =
check_recipient_access hash:⇒
/etc/postfix/recipient_access,reject_unauth_destination
```

d. To switch to command mode, press **Esc**.

e. Save and close the file.

f. Using the `vi` editor, open the `sender_access` file.g. To discard messages after accepting them, type `junk@junkmail.com`
ERROR: 550 MAIL DISCARDEDh. To switch to command mode, press **Esc**.

i. Save and close the file.

j. To build the access database with respect to the sender, enter **postmap**
sender_access < sender_accessk. Using the `vi` editor, open the `recipient_access` file.l. To reject Eric's mail, enter
eric@ourglobalcompany.com REJECTm. To switch to the command mode, press **Esc**.

n. Save and close the file.

o. To build the access database with respect to the recipient, enter **postmap**
recipient_access <
recipient_access

p. Restart the postfix service.

LESSON 13

-
- | | |
|---|----------------------|
| 6. Check whether the message from junkmail.com is rejected. | q. Clear the screen. |
|---|----------------------|
-
- | | |
|--|--|
| 7. Check whether the recipient, Eric, is not permitted to receive mail messages. | a. Switch from the system labeled srvA to the system labeled srvB. |
| | b. On the system labeled srvB, enter
<code>telnet ourglobalcompany.com 25</code> |
| | c. Enter <code>HELO ourglobalcompany.com</code> |
| | d. Enter <code>MAIL FROM:</code>
<code>junk@junkmail.com</code> |
| | e. Enter <code>RCPT TO:</code>
<code>chris@ourglobalcompany.com</code> |
| | f. Observe that the error message, "451 4.3.5 Server configuration error", is displayed indicating that the junk mail filter is working. |
| | g. Quit the Telnet connection. |
-
- | | |
|--|---|
| 7. Check whether the recipient, Eric, is not permitted to receive mail messages. | a. On the system labeled srvB, enter
<code>telnet ourglobalcompany.com 25</code> |
| | b. Enter <code>HELO ourglobalcompany.com</code> |
| | c. Enter <code>MAIL FROM:</code>
<code>chris@ourglobalcompany.com</code> |
| | d. Enter <code>RCPT TO:</code>
<code>eric@ourglobalcompany.com</code> |
| | e. Observe that the error message, "Recipient address rejected: Access denied," is displayed. |
| | f. Quit the telnet connection. |
| | g. Clear the terminal screen. |
-
-

TOPIC B

Control Internet Services

In the last topic, you configured email services. There are numerous services and benefits that the Internet offers. This has made the Internet a necessity in almost all organizations. In this topic, you will control Internet services.

Internet services are crucial for the effective functioning of businesses. Any disruption or problems in Internet services could paralyze regular work and cost organizations dearly. As a Linux system administrator, it is your primary responsibility to ensure that Internet services are running without any problems all the time.

The xinetd Daemon

The *xinetd* daemon controls system services on a network and is based on the client-server architecture. Various services are listed in the configuration files of *xinetd*. When the daemon receives a request from a port for a particular service, it checks with the configuration files and then starts the appropriate server containing the service. This enables faster service management over the network because requests are handled immediately. Services that are managed by *xinetd* include file sharing, Telnet, rsync, and time management. The settings for these services can be controlled using the `/etc/xinetd.conf` file or the service-specific files found in the `/etc/xinetd.d` directory.

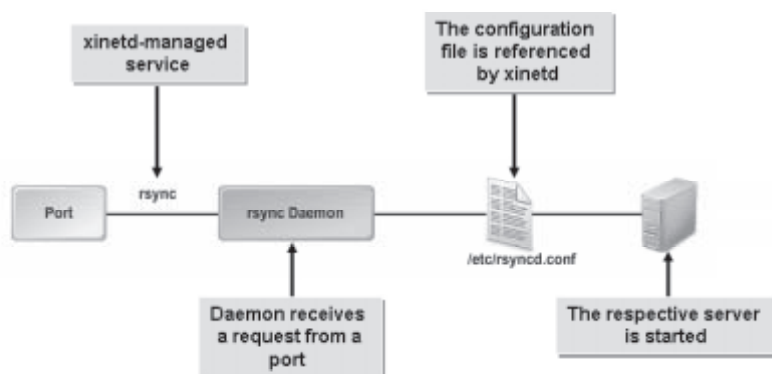


Figure 13-8: The *xinetd* daemon controls services on clients and servers.

Telnet

Definition:

Telnet is a terminal emulation protocol that enables a user on a site to simulate a session on a remote host. In other words, it allows a user to log in to another computer over a network. It does this by translating keystrokes from the user's terminal into instructions recognized by the remote host, and then carrying the output back to the user's terminal and displaying it in a format native to the remote host. This service is transparent; it gives users the impression that their terminals are directly attached to the remote host. The remote computer needs to have a Telnet server, and the user's computer needs to have a Telnet client.

Example:

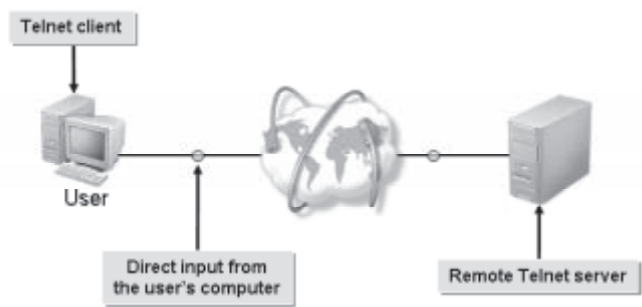


Figure 13-9: A Telnet client communicating with a remote Telnet server.

Disadvantages of Telnet

Telnet is not a very secure protocol because it transmits passwords as plain text. Telnet has largely been replaced by SSH because it offers better security.

The /etc/xinetd.conf File

The /etc/xinetd.conf file is the configuration file for the xinetd daemon and contains a list of services managed by the daemon. It is referenced by the daemon each time a request is sent for a service to be started or stopped. The file is divided into different parts for each of the service containing the service settings. Services can be single threaded or multithreaded.

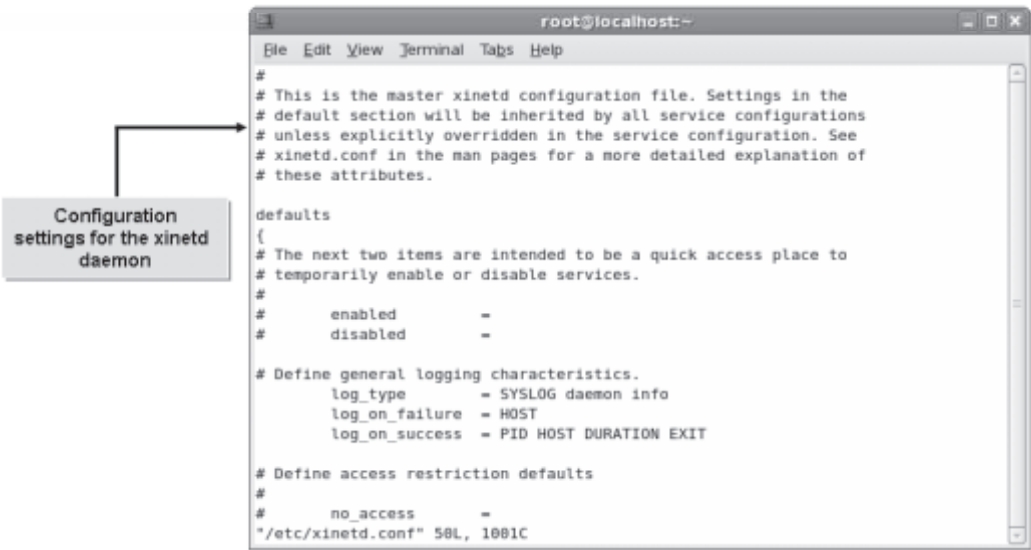


Figure 13-10: The xinetd.conf file with its various configuration settings.

The /etc/xinetd.conf file can be configured according to user requirements using a number of options. Some of the frequently used options are listed in the table.

Option	Enables You To
service	Specify the service name.

Option	Enables You To
wait	Specify whether the service is single threaded or multithreaded.
user	Specify the UID for the process running on the server.
server	Specify the executable that is to be launched on the server when the service is invoked.
disable	Specify whether a service is enabled or disabled.

Syntax

The syntax for specifying services in the xinetd configuration files is `{attribute} {assignment operator} {value}`.

The libwrap.so Libraries

The libwrap.so files are libraries that are linked to services controlled by the xinetd daemon. There are three main library files: libwrap.so, libwrap.so.0, and libwrap.so.0.7.6. These files, found in the /usr/lib directory, control the TCP services and additional network access settings, including the settings found in the network access configuration files.

The /etc/xinetd.d Directory

The /etc/xinetd.d directory contains configuration scripts for services managed by xinetd. Some of the services listed in this directory are ftp, kerberos, and rsync. Each service can be individually configured using the configuration file found in this directory. The options in the service configuration files are similar to those found in the /etc/xinetd.conf file.

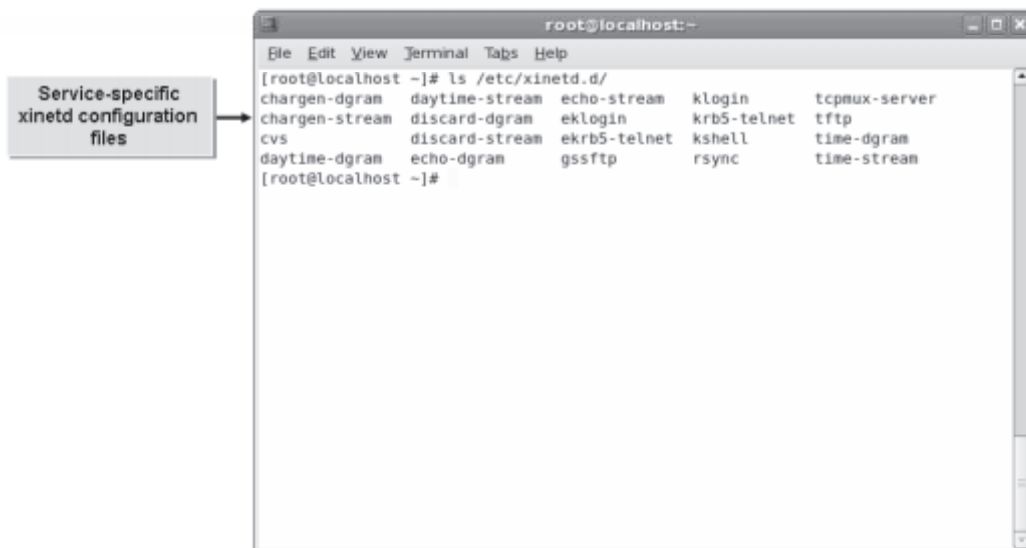


Figure 13-11: The xinetd.d directory contains configuration files for xinetd-managed services.

xinetd Access Controls

The `xinetd` daemon has a set of functions for controlling access to services managed by it. These access controls are of two types: host based and time based.

Access Control Type	Description
Host based	Host-based access controls are implemented by restricting hosts in the <code>xinetd</code> service configuration file through the <code>no_access</code> and <code>only_from</code> options. Host Pattern Access Controls are used to specify host patterns when host-based access controls are implemented. Hosts may be specified in the form of their IP addresses, netmask ranges, network names, or hostnames.
Time based	Time-based access controls are implemented by adding the <code>access_times</code> option to the service configuration file.

Service and Application Access Controls


Service access controls and *application access controls* are daemons used for restricting access to certain important services and applications, such as those that control network connections and security policies. Examples of these daemons are `squid` and `httpd`. These daemons restrict access by referring to the hostnames or IP addresses of systems listed in the `libwrap.so` file or the `xinetd` configuration files. If systems have the required permission, the daemons will permit them to access the protected services and applications.

How to Control Internet Services

Procedure Reference: Configure Services Managed by `xinetd`

To configure services managed by `xinetd`:

1. Log in as root.
2. To list the services managed by the `xinetd` daemon, enter `ls -l /etc/xinetd.d/`.

 In the older versions of Linux, the `/etc/xinetd.d/*` file was referred to as the `/etc/inetd.d/*` file.
3. Manage the `xinetd` daemon at system startup.
 - To make sure that the `xinetd` daemon is configured to start in the desired runlevel, enter `chkconfig --list xinetd`.
 - To update the runlevel configuration of the `xinetd` daemon, enter `chkconfig --level {levels} xinetd {on/off}`.
 - To manage the status of the `xinetd` daemon, enter `service xinetd {start/stop/status/restart/reload}`.
4. Manage services controlled by the `xinetd` daemon.

- To enable or disable the specified service at system startup, enter `chkconfig {service name} {on/off}` or;
- Manage the service using configuration files found in the `/etc/xinetd.d` directory.
 - a. To edit the service-specific configuration file, enter `vi /etc/xinetd.d/{service configuration file}`.
 - b. To disable or enable the service, edit the “`disable = {yes/no}`” line.
 - c. To define the service-specific settings that override the global settings for all services managed by the `xinetd` daemon, edit `<attribute> <assignment operator> <value> <value>`.
 - d. Save and close the file.
 - e. To reload the `xinetd` daemon with the applied changes, enter `service xinetd reload`.

Procedure Reference: Define the Global Settings in the `/etc/xinetd.conf` File

To define the global service settings in the `/etc/xinetd.conf` file:

1. Log in as root.
2. To edit the `xinetd` daemon configuration file, enter `vi /etc/xinetd.conf`.
3. To define the global settings for all services managed by `xinetd` daemon, edit `{attribute} {assignment operator} {value} {value}`.
4. Save and close the file.
5. To apply the changes, enter `service xinetd restart`.

Procedure Reference: Configure Access Control for `xinetd` Managed Services

To configure access control for `xinetd` managed services:

1. Log in as root.
2. Define service-specific access control in the `/etc/xinetd.conf` file.
 - a. To edit the service-specific configuration file, enter `vi /etc/xinetd.d/{service configuration file}`.
 - b. To define the remote hosts for which the particular service is available, type `only_from = {list of IP addresses}`.
 - c. To define the remote hosts for which the particular service is unavailable, type `no_access = {list of IP addresses}`.
 - d. To define the time intervals when the service can be accessed, type `access_times = {hour:min-hour:min}`.
3. Save and close the file.
4. To apply the changes and restart the `xinetd` daemon, enter `service xinetd restart`.

Procedure Reference: Monitor Sendmail, Postfix, or Qmail Mail Servers Using Telnet

To monitor Sendmail, Postfix, or Qmail mail servers using Telnet:

1. Connect to the SMTP server on port 25.
`telnet {server's IP address} 25`
2. Send an email message using Telnet and observe the results to ensure that the SMTP server is properly functioning.
 - a. To specify your hostname, enter `HELO {server name}`.
 - b. To specify the sender's email address, enter `MAIL FROM: email address`.
 - c. To specify the recipient's email address, enter `RCPT TO: email address`.
 - d. Enter `DATA`.
 - e. Enter the subject and message. Terminate the message with a period.

ACTIVITY 13-2

Enabling Service Access Controls

Before You Begin:

1. On `srvA`, you have logged in as root in the CLI.
2. To navigate to the root directory, enter `cd /root`.
3. To clear the terminal screen, enter `clear`.

Scenario:

You are working as a system administrator at OGC. Your organization has several branches, and you want to enable employees working in different branches to communicate with each other. You want to use the telnet protocol to transfer files and add tunneling capability. In addition, you have to configure the service to start automatically during system startup. Finally, you also have to ensure that the service is inaccessible from the system with IP address 192.168.0.205 because it will be accessed by unauthorized users.

What You Do	How You Do It
1. Install the telnet service on the system.	<ol style="list-style-type: none"> To install the telnet service, enter yum localinstall /rhelsource/Server/telnet* Observe that Transaction Summary displays that one package is to be installed. Also, observe that the total download size is 35 k. To download and install the package, enter y Observe that the message "Complete" is displayed indicating that the telnet service is installed.
2. Enable the telnet server.	<ol style="list-style-type: none"> To open the telnet configuration file, enter vi /etc/xinetd.d/telnet Observe that the default configuration entries are displayed. Also, observe that the service is disabled as indicated by disable=yes. To navigate to the "disable = yes" line, enter /dis Switch to insert mode. Change disable = yes to disable = no
3. Enable access control for the telnet service.	<ol style="list-style-type: none"> On a new line, press Tab. Enter only_from and press Tab. To allow the service to be accessed only from 192.168.0.0, enter = 192.168.0.0/24 Press Tab and enter no_access. To deny access to the service for all users from 192.168.0.205, press Tab and enter = 192.168.0.205 Switch to command mode. Save and close the file.

LESSON 13

4. Configure xinetd to start at system boot.
 - a. To start the xinetd service, enter **service xinetd start**
 - b. To enable the xinetd service to start at system startup, enter **chkconfig xinetd on**
 - c. Clear the terminal screen.
-

Lesson 13 Follow-up

In this lesson, you configured email services and controlled Internet services. Now, you will be able to implement a cost-effective solution for communication, sharing, and transfer of resources across a network.

1. Which mail retrieval protocol would you configure in your organization? Why?
2. What are the advantages of implementing sendmail in your organization?

LESSON 14

Securing Linux

Lesson Time*1 hour(s), 30 minutes*

In this lesson, you will implement measures to secure a Linux system.

You will:

- Implement encryption services.
- Secure user accounts.
- Implement iptables.
- Implement auditing for security purposes.
- Describe the Intrusion Detection System.

Introduction

In the last lesson, you configured basic Internet services. All networked services, no matter how basic, need to be secured. Poor security can lead to damage or loss from disgruntled employees, hackers, or competitors. In this lesson, you will secure a Linux system connected to a network.

To properly secure a Linux system, an administrator has to understand how different threats affect the system. Specific security measures that allow the administrator to control the transfer of sensitive data and restrict unauthorized users from accessing the network need to be implemented.

This lesson covers all or part of the following CompTIA Linux+ Powered by LPI certification objectives:

- Topic A:
 - Objective 110.2, Objective 110.3
- Topic B:
 - Objective 105.1, Objective 107.1, Objective 110.1, Objective 110.2
- Topic E:
 - Objective 110.1

TOPIC A

Examine the Basics of System Security

In the previous lesson, you worked with the Internet and email services. These services are prone to threats from hackers, which can cause serious problems. A security breach in an organization's network cannot be compromised because sabotage or data theft could affect business badly. These instances can be avoided by securing the systems and sending data in a secured format that can be comprehended only by the user to whom the data is directed. In this topic, you will examine the basics of system security.

Computer security is a critical part of business strategy, and organizations continually demand new levels of protection. On a network, there are various web and mail services that can be implemented. Though these services facilitate data transfer, there is always the risk of data theft associated with them. Without proper security and encryption mechanisms governing these services, transferring sensitive data securely is impossible.

Keys

While logging in to a remote machine, the private and public keys are combined by the remote server for verification. A user can log in and transfer files only if the keys match. Authenticity is established by the remote server, which then grants the necessary permissions.

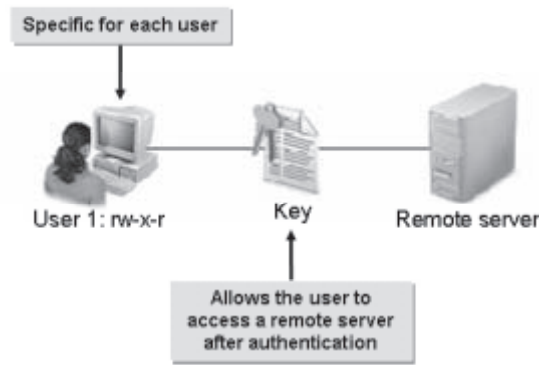


Figure 14-1: Securing data using a key.

Keys are of two types: public and private.

Key Type	Description
Public	A <i>public key</i> is the key that is transmitted to the destination server along with the request. This is compared with the private key of the destination. Only when these two are related, the user is authenticated.
Private	A <i>private key</i> is retained on the local system and is not transmitted to the destination server. Data is sent to the user along with the sender's public key. The user can access data only when the private key of the user is authenticated by the public key of the sender.

Authentication

Authentication verifies that users are who they say they are. In data communication, authenticating a sender is necessary to verify that the data came from the right source. A receiver is authenticated as well, to verify that the data is going to the right destination.

There are several methods for ensuring authentication.

Method	Description
The <i>known_hosts</i> file	When you connect to a remote host, the host sends your public host and server keys for authentication. Your system looks up the <i>known_hosts</i> file to locate an entry for the host's keys, and if an entry is found, you will be granted access.
The <i>SSH</i> server	A server that automatically generates public host and server keys for authentication purposes. Server keys are automatically regenerated every hour to ensure security.

Method	Description
<i>Challenge Handshake Authentication Protocol (CHAP)</i>	A security authentication protocol that encrypts the user name and password information using a key and transmits them over the network. CHAP is supported on lines using Point-to-Point Protocol (PPP) encapsulation.
<i>Password Authentication Protocol (PAP)</i>	A security authentication protocol for logging in to a network. With PAP, the unencrypted user name and password are transmitted over the network to the server. This information is checked against a table containing user name and password pairs of all the users on the network. PAP is supported only on PPP lines.
<i>Kerberos</i>	A network authentication service that is used by client/server applications. Kerberos creates a key, or ticket, for each user logging in to the network. The tickets are embedded along with the message to identify the sender.

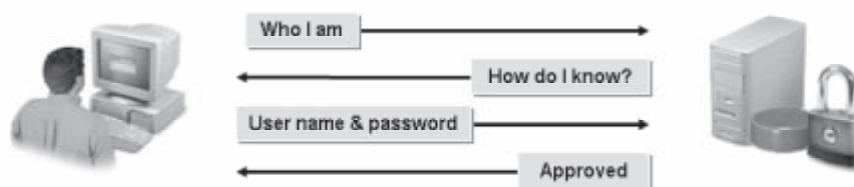


Figure 14-2: *The authentication process.*

Authentication Factors

The number of factors that are used to show the identity of a user through authentication determines how effective authentication can be. The three types are:

- One-factor authentication, which provides what you know, such as a password or PIN. It is based on recalling a piece of information from your memory or by writing the information down. This type of authentication is the least effective.
- Two-factor authentication, which combines what you have with what you know. For example, your ATM card combined with the PIN provides access to your bank account.
- Three-factor authentication, which also provides proof of the user's identity through biometrics. It uses physiological identification characteristics such as fingerprints, voice recognition, or signature recognition. This is the best type of authentication.

Biometric Authentication

To increase the level of reliability of systems and ease of use to users (beyond password authentication), biometric authentication can be introduced. When this type of system is added to an authentication scheme, it is considered to be a strong authentication. The designation of strong is given because a user is not only identified digitally, but by his or her physiological characteristics, through fingerprint scanning, iris scanning, or hand geometry.

Encryption

Encryption is a method of controlling user access to information, by configuring data to appear as codes that cannot be interpreted by unauthorized users. To authorized users, though, this data appears in its original form. Passwords can also be used to protect data along with encryption. Various protocols, such as SSH, SSL, and SECURENET, are used to implement encryption on a network.

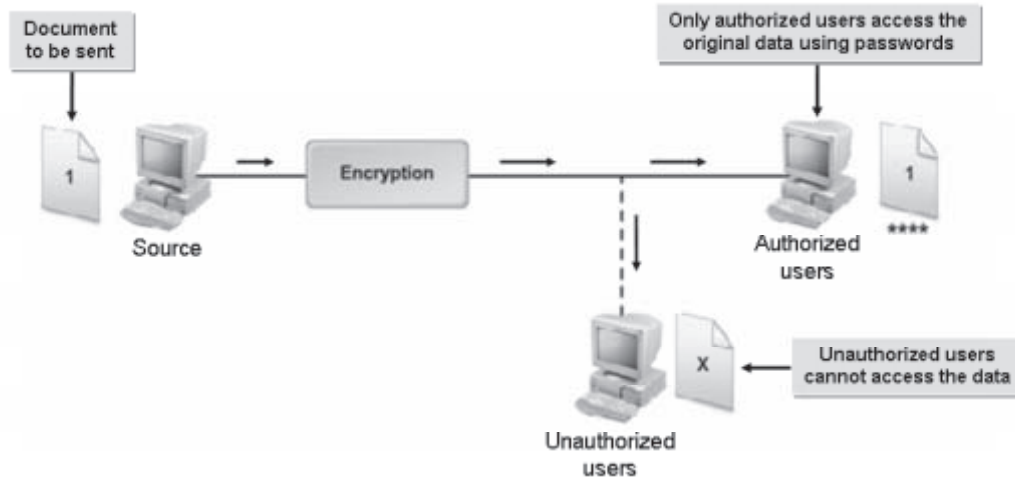


Figure 14-3: Securing data using encryption.

Encryption Solutions

Authorized users of encrypted computer data must have the key that was used to encrypt the data in order to decrypt it. Different solutions are available for encrypting data using specific *algorithms*.

Solution	Description
<i>Blowfish</i>	<p>A symmetric block cipher that provides strong encryption and uses key sizes up to 56 bytes (a 448-bit key). Its features include:</p> <ul style="list-style-type: none"> • Strong key support, handling, and cryptography. • Security to wipe files and clear empty disk space.
<i>3DES</i>	<p>A block cipher algorithm (pronounced “triple dez”) that can encrypt and decrypt data using a secret key. 3DES uses three stages of <i>DES</i> (<i>Data Encryption Standard</i>), making it a very secure option. Anything encrypted by DES encryption has 72,000,000,000,000,000 (or 72 quadrillion) possible keys.</p>
<i>MD5</i>	<p><i>Message-Digest algorithm 5 (MD5)</i> is a command-line utility that generates and verifies <i>message digests</i> (digital signatures) using the MD5 algorithm.</p> <p>The MD5 algorithm is intended for digital signature applications, where a large file must be compressed in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem.</p> <p>MD5 is also used to check the integrity of files.</p>

Random Number Generation

Random number generation is an encryption method in which the kernel is used to generate random numbers that are assigned to files before transfer. Only when the numbers are matched by the recipient is the transfer completed. The algorithm that governs random number generation is the *Pseudo Random Number Generation (PRNG)* algorithm. In Red Hat Linux, the kernel files, `/dev/random` and `/dev/urandom`, act as random number generators. Using the concept of permutations and combinations, these kernels are able to generate numbers with millions of digits from a single source number.

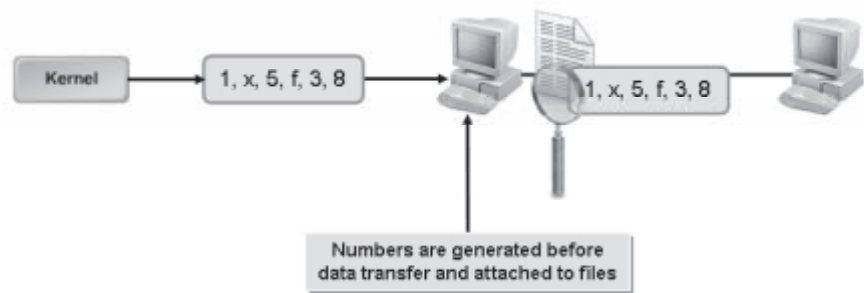


Figure 14-4: Securing data using the random number generation method.

Cryptographic Hashes

Cryptographic hashes are used in an encryption method in which arbitrary data is encapsulated within a fingerprint that is attached to a file. A fingerprint is a fixed string called the hash value, checksum, or message digest. The data in the file can be checked for authenticity by verifying the hash value. When modifications are made to a file, its hash value also changes. Various algorithms, such as MD2, MD5, SHA, and SHA1, are used to implement cryptographic hash functions.

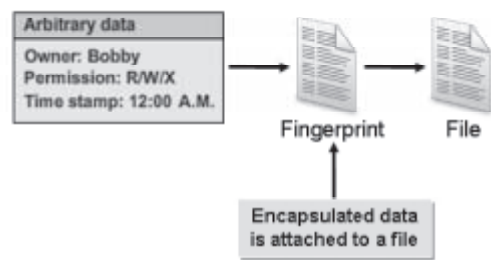


Figure 14-5: Securing data using the cryptographic hashing method.

Various utilities are used to check the hash values of files.

Utility	Enables You To
sha1sum	Check files for improper sha1 checksums. The syntax of this utility is <code>sha1sum --check {file name}</code> .
md5sum	Check files for improper md5 checksums. The syntax of this utility is <code>md5sum --check {file name}</code> .

Symmetric Encryption

Symmetric encryption is carried out using only a single key, which is used for both encryption and decryption. Various utilities are used to perform symmetric encryption.

Utility	Used To
<code>passwd</code>	Change the login password. Users who are logged in can change only their login password, and not that of other users. However, this does not apply to the root user. When you type the <code>passwd</code> command at the command prompt, you are asked to enter your current password and then the new password you want to set. The new password is effective the next time you log in to the system.
<code>gpg</code>	Encrypt messages using the GNU Privacy Guard (GnuPG) encryption system. This utility has various commands and options. The syntax of this utility is <code>gpg [options] {command} {arguments}</code> .
<code>openssl</code>	Encrypt and decrypt messages using the SSL protocol through creation of keys, certificates, and signatures. The syntax of this utility is <code>openssl {command} [options] {arguments}</code> .
<code>make</code>	Generate digital certificates and key pairs. This command must be run from the <code>/etc/pki/tls/certs/</code> directory. The syntax of this utility is <code>make {key file digital certificate}</code> .

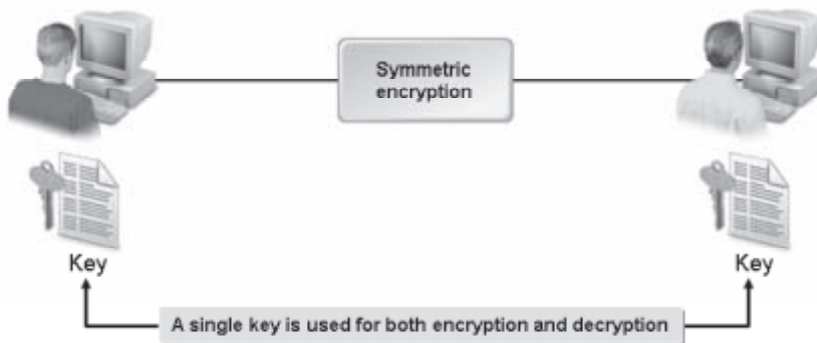


Figure 14-6: Key generation in symmetric encryption.

Asymmetric Encryption

Asymmetric encryption is carried out using two keys in the form of key pairs. While one key is used for encryption, the other key is used for decryption.

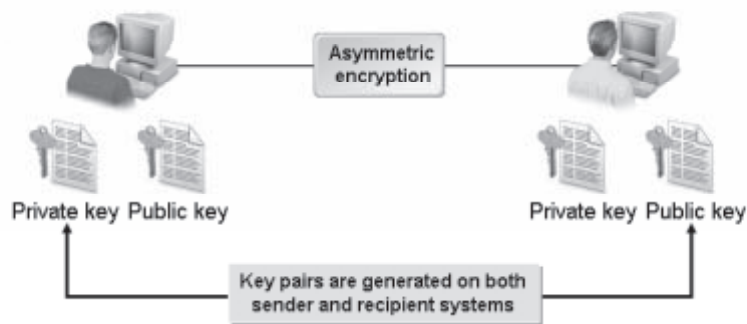


Figure 14-7: Key generation in asymmetric encryption.

There are two main protocols involved in asymmetric encryption: protocol 1 and protocol 2. Only one protocol can be implemented at a time.

Protocol	Description
Protocol 1	<p>Only one key is exchanged between a sender and a recipient.</p> <ol style="list-style-type: none">1. The recipient first generates a key pair, which contains a public key and a private key.2. The request is then sent to the sender in an encrypted form along with the public key of the recipient. The private key is retained with the recipient.3. The sender receives the request, authenticates the public key sent by the recipient, and then returns the requested information in the encrypted form along with the public key of the recipient.4. The recipient receives the information along with its public key and decrypts it by authenticating the public key with its private key.
Protocol 2	<p>Digital signatures are used along with key encryption. A digital signature is a unique ID created when a message digest of the sender is encrypted.</p> <ol style="list-style-type: none">1. The sender first generates a key pair, which contains a public key and a private key. Using the private key and the message digest, the sender generates a digital signature.2. The public key is transmitted to all the systems on a network. The request is then sent by the recipient to the sender.3. The sender receives the request and returns the information in an encrypted form along with its digital signature.4. The recipient receives the information and decrypts it by authenticating the digital signature of the sender with its public key.

Rogue Public Keys


Rogue public keys are generated by unauthorized users to bypass public key cryptography. These are used to decrypt information that they are not supposed to access.

Generation of rogue keys can be prevented by using public key fingerprints, forming trusted groups, and issuing digital certificates through trusted certificate authorities.

Digital Certificate Types

A digital certificate is a method of symmetric encryption. Two main types of digital certificates are available.

Certificate Type	Description
Certificate Authority	<i>Certificate Authority certificates</i> are generated by a common and trusted Certificate Authority (CA) on receiving a certificate signature request (csr). The advantage of using this method is that generation of rogue digital certificates can be prevented.
Self-signed	<i>Self-signed certificates</i> are generated by users themselves and contain the public key of the user as the signature. Therefore, any user can create a self-signed certificate. However, this certificate does not provide guarantee about the identity of the user or the organization.

 The X.509 format is a standard format for public key certificates.

Package Integrity

Each package in Linux is assigned a public key, which is installed along with the package. *Package integrity* is the method of checking packages for these public keys to ensure that the package has come from a trusted vendor. It is necessary to perform a package integrity test before installing a package because installing a package from an unreliable source may lead to improper installation and virus attacks. The `yum` command always installs packages along with their public keys from the Red Hat online repository.

The `rpm` command can be used to check file integrity.

Command	Enables You To
<code>rpm --verify {package name}</code>	Check whether the package is installed or not.
<code>gpg --import /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat*</code>	Import public keys to the rpm database.
<code>rpm --checksig {package name}</code>	Check whether the package has valid signatures.
<code>rpm --addsign {package name}</code>	Assign valid signatures to the package.

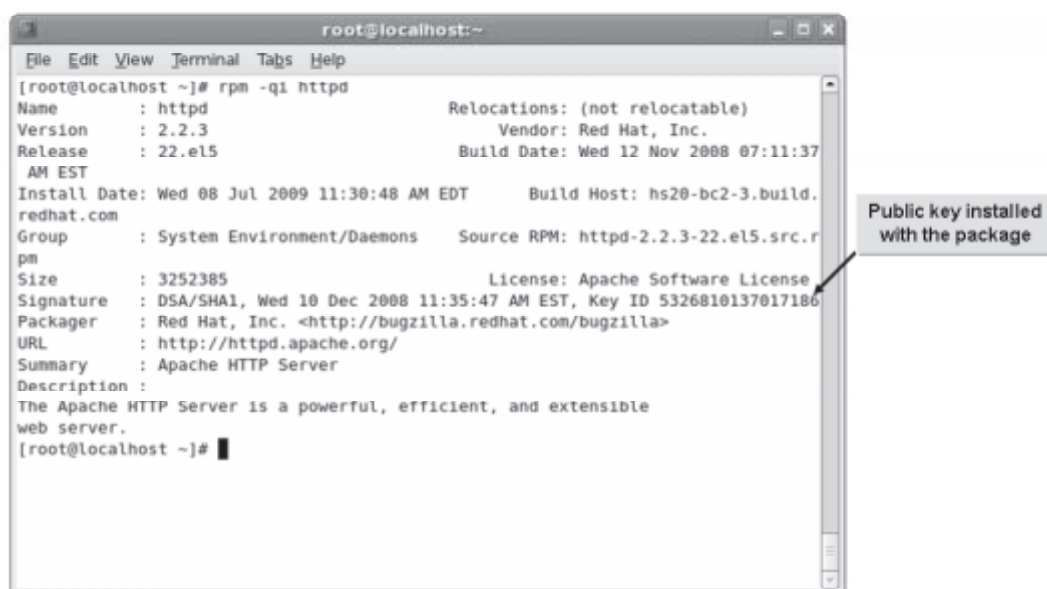


Figure 14-8: Package information displaying the installed public key.

RADIUS

Remote Authentication Dial In User Service (RADIUS) is a client/server protocol that facilitates centralized authentication, authorization, and accounting over a network. User information is stored in a central database, which is shared by all remote servers. When a user sends a request to access a service or resource, RADIUS enables remote access servers to communicate with a central server to verify the authenticity of the user. It usually utilizes the user's login and password, stored in the `/etc/passwd` file on the server, to verify the user's credentials. It allows secure transmission of passwords by encrypting them with the MD5 algorithm. The RADIUS server is widely used by Internet Service Providers (ISPs).

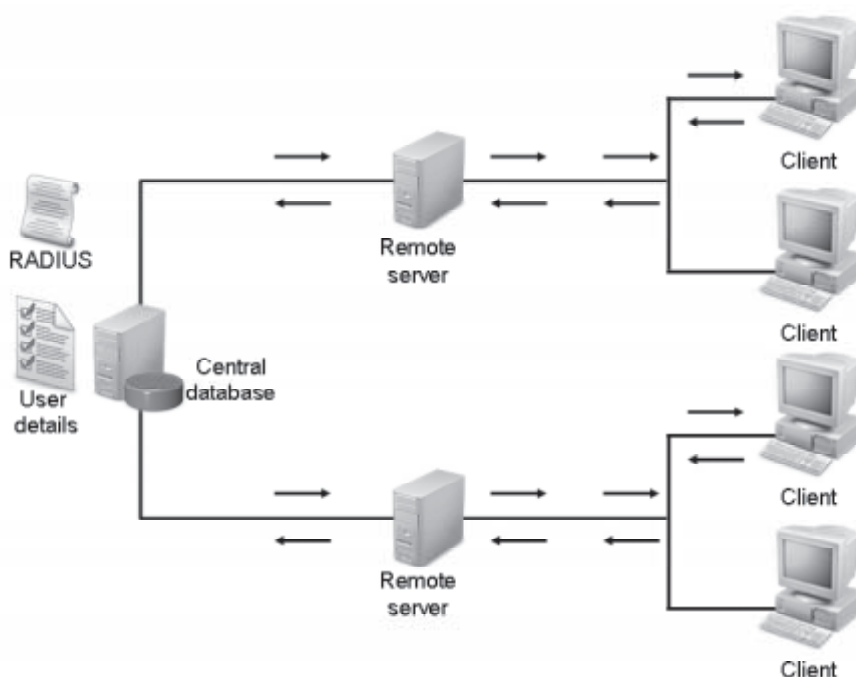


Figure 14-9: The RADIUS protocol providing authentication services on a network.

The RADIUS Server as a Network Access Server

When a network contains several remote access servers, you can configure one of the servers as a RADIUS server and all other servers as RADIUS clients. The RADIUS clients will pass all authentication requests to the RADIUS server for verification. User configuration, remote access policies, and usage logging can be centralized on the RADIUS server. In this configuration, the remote access server is generically known as the Network Access Server (NAS).

TCP Wrappers

Definition:

TCP wrappers are protection layers that define the host computers that are allowed to connect to some network services and those that are not. The TCP wrappers package consists of the `/lib/libwrap.so.0` library. A TCP wrapped service is compiled using the `libwrap.so.0` library. TCP wrappers operate separately from the network services protected by them.

Example:

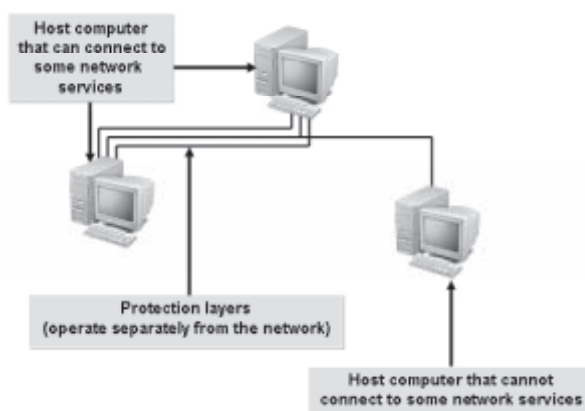


Figure 14-10: *TCP wrappers with protection layers.*

How to Implement Encryption Services


Procedure Reference: Configure Encryption

To configure encryption:

1. Log in as root.
2. To open the file, enter `vi /etc/{application}/{configuration file}`.
3. Locate the line that contains the encryption details.
4. If necessary, uncomment the line.
5. Modify the line to change the type of encryption.
6. Save the file and exit from the editor.
7. Restart the daemon service of the application or device for the changes to apply.

Procedure Reference: Implement Cryptographic Services

To implement cryptographic services:

1. Log in as root.
 2. Implement cryptographic services.
 - To generate a random number, enter `openssl rand {options} {number of pseudo-random bytes}`.
 - Generate a message digest.
 - To compute and check the SHA1 message digest, enter `shasum [options] {file name}`.
 - To compute and check the MD5 message digest, enter `md5sum [options] {file name}`.
 - To output the message digest of a supplied file, enter `openssl dgst {message digest options} {file name}`.
 - Implement symmetric encryption using the `gpg` command.
 - To encrypt a file with symmetric encryption, enter `gpg --symmetric {file name}`.
 - To decrypt an encrypted file using the `gpg` command, enter `gpg -d {file name}`.
-  `~/.gnupg` is the directory that stores the private and public keys created using the `gpg` command.
- Implement encryption using the `openssl` command.
 - a. To encrypt the file and store the output in another file, enter `openssl enc -e -salt -{bf/des3/cast5-cbc} -in {absolute or relative path of file to be encrypted} -out {absolute or relative path of encrypted file}`.
 - b. Enter the symmetric encryption password when prompted.
 - c. To decrypt the file and store the decrypted data in another file, enter `openssl enc -d -{bf/des3/cast5-cbc} -in {absolute or relative path of encrypted file} -out {absolute or relative path of decrypted file}`.
 - d. Enter the encryption password when prompted.

Procedure Reference: Verify Package Integrity Using the `rpm` Command

To verify package integrity using the `rpm` command:

1. Log in as root.
2. Verify package integrity.
 - To report files that differ from the original `rpm` version, enter `rpm --verify {package name}`.
 - To import GPG keys to add them to packages, enter `rpm --import /etc/pki/rpm-gpg/RPM-GPG-KEY-*`.
 - To check whether the `rpm` package was packaged by Red Hat, enter `rpm --checksig {package name}`.

Procedure Reference: Generate Digital Certificates

To generate digital certificates:

1. Log in as root.
2. Generate keys using the `openssl` command.
 - a. To generate a public or private key pair, enter `openssl genrsa -out {absolute or relative path of key file} {key size}`.
 - b. To generate a certificate signature request, enter `openssl req -new -key {absolute or relative path of key file} -out {absolute or relative path of certificate request file}`.
 - c. Enter required information such as the country name, state, city, organization name, organizational unit name, server name, email, and if necessary, a challenge password and the optional company name.
 - d. To generate a self-signed certificate, enter `openssl req -new -key {absolute or relative path of key file} -out {absolute or relative path of certificate file} -x509`.
 - e. Enter required information such as the country name, state, city, organization name, organizational unit name, server name, email, and if necessary, a challenge password and the optional company name.
3. Generate digital certificates using the `make` command.
 - a. To generate a public or private key pair, enter `make -C /etc/pki/tls/certs {file name}.key`.
 - b. To generate a certificate signature request, enter `make -C /etc/pki/tls/certs {file name}.csr`.
 - c. To generate a certificate, enter `make -C /etc/pki/tls/certs {file name}.crt`.
 - d. To generate a key and a certificate in one file, enter `make -C /etc/pki/tls/certs {file name}.pem`.

Procedure Reference: Configure TCP Wrappers to Allow or Deny Services

To configure TCP wrappers to allow or deny services:

1. Log in as root in the CLI.
2. Allow services to a particular IP or domain address.
 - a. Enter `vi /etc/hosts.allow`.
 - b. Enter `{service name}: {ip/domain address}`. For example, `sendmail: 192.168.1.1` means that the TCP wrapper should allow the sendmail service request from the specified IP address.
 - c. Save and close the file.
3. If desired, deny services to a particular IP or domain address.
 - a. Enter `vi /etc/hosts.deny`.
 - b. Enter `{service name}: {ip/domain address}`. For example, `sendmail: 192.168.1` means that the TCP wrapper should deny the sendmail service request from the specified IP network.

c. Save and close the file.

ACTIVITY 14-1

Configuring Encryption

Before You Begin:

- 1. On srvA, you have logged in as root in the CLI.
- 2. The first terminal is displayed.

Scenario:

While analyzing log files, you detect failed attempts to access the SSH service. You decide to configure the Linux server so that it encrypts the information with Blowfish before transmitting data using SSH.

What You Do	How You Do It
1. Edit the /etc/ssh/ssh_config file.	<ul style="list-style-type: none">a. To open the file, enter <code>vi /etc/ssh/ssh_config</code>b. Locate the text "Cipher."c. Uncomment the line "# Cipher 3des."d. On the same line, delete "3des."e. To switch to insert mode, press <code>I</code>.f. Press the Spacebar and type blowfishg. To save and close the file, press Esc and enter <code>:wq</code>
2. Restart the sshd service.	<ul style="list-style-type: none">a. Enter <code>service sshd restart</code>b. To check whether the service is started, enter <code>service sshd status</code>c. Verify that the openssh-daemon is running.d. To clear the terminal screen, enter <code>clear</code>

TOPIC B

Secure User Accounts

You are now familiar with encryption and basic system security. The next step is to provide users with a secure computing environment. In this topic, you will secure user accounts.

Given the reputation that Linux has as a secure operating system, there may be an inherent tendency to take a casual approach to user security. However, as a Linux administrator, it is important to institute organizational policies that help establish best practices in your Linux user community. By doing so, you will limit the potential for disasters, especially as your company user base grows.

Environment Files

In Linux, several environment files can be customized.

File	Description
/etc/hosts.allow	Allows access to certain services and hosts.
/etc/hosts.deny	Denies access to certain services and hosts.
/etc/limits	Limits users' resources when a system has shadow passwords installed.
/etc/login.defs	Sets user login features on systems with shadow passwords.
/etc/passwd	Displays the user name, real name, home directory, encrypted password, and other information of a user.
/etc/securetty	Identifies secure terminals from which the root user is allowed to log in to.
/var/log/secure	Tracks user logins. It is recommended to check this file periodically.

The /etc/login.defs File

The /etc/login.defs file is used with shadow passwords to set the initial path and other parameters, including how often a user must change passwords and what is acceptable as a password.

Login Levels

In Linux, you can provide root-level or user-level access to resources. By default, the root user has login privileges to all information on the system, but other users have limited login privileges.

Login Level	Description
Root login	<p>Root user is considered a specific user account, with a UID of 0. It has privileges that no other user on the system has.</p> <p>Specifically, the root user can navigate anywhere on the system, change any file, and manipulate system controls, including user accounts, storage devices, and kernel parameters.</p> <p>The system administrator(s) will generally have his or her own user accounts with normal user privileges, and the root account. As a rule of thumb, you should do as much as possible under your UID before working from the root user account.</p>
User login	<p>User accounts must be created with security in mind. The user name, or login ID, and the password are stored in two different files, <code>/etc/passwd</code> and <code>/etc/shadow</code>, and are set up with restricted access rights for added security.</p> <p>The user account file, <code>/etc/passwd</code>, is set up to be read-only by everybody except the root user.</p>

Alias for the Root User

If you are using the Bash shell, you can create an alias for root as a precautionary measure. An alias, in this case, is an entry in the `.bashrc` file where you can define additional actions for specific default commands. For example, the `rm` command, which is used for removing or deleting files, can be given an alias that prompts you for additional information, based on the criteria you set.

The su Command

The *substitute or switch user* (`su`) command is used to change the ownership of a login session without logging out. It is generally used to switch ownership between an ordinary user and a root user, to change access permissions for administrative work.



Figure 14-11: Switching users using the *su* command.

The Login Shell vs. the Non-Login Shell

A login shell is a shell that is created during a user login. On the other hand, a non-login shell is a shell that you can invoke from within a login shell. For example, running the `su` command from a login shell, invokes the non-login shell. However, the `su -` command can be used to run commands in the login shell. GNOME terminals and executed scripts are non-login shells. The `logout` command can be run only in login shells, whereas the `exit` command can be run in both the login and non-login shells.

The `id` Command

You can use the `id` command to view user identities. This allows you to identify the owner of the current login session.

The `sudo` Command

The *super user do* (`sudo`) command allows users to run programs with the security privileges of the root user. It prompts you for your password and confirms your request to execute a command by checking the `/etc/sudoers` file, which is configured by the system administrator. The `sudo` command allows system administrators to give certain users or groups access to some or all commands without users knowing the root password. It also creates a log of all commands and arguments used, to maintain a record.



Figure 14-12: Using the *sudo* command to perform tasks with root privileges.

Syntax

The syntax of the *sudo* command is `sudo {command name} {options}`. For example, `sudo shutdown -h now` will begin a system shutdown, if a user has permission to access the shutdown command via *sudo*.

After executing the *sudo* command, the user will be prompted for his or her password. This is an extra security measure to ensure that unauthorized users cannot access the *sudo* command from authorized users' login session without their knowledge.

Password Policies

A *password policy* is a set of guiding principles that help form effective passwords. A password policy divides users of a system into various categories with differing levels of access to resources.

Guidelines:

A password policy may have the following rules:

- Passwords need to be at least seven characters long.
- Passwords must be made up of numbers, upper and lowercase letters, and special characters such as punctuation.
- Passwords must not be a recognizable English word.
- Passwords must be changed every three months.
- Password policies encourage users to avoid writing down their passwords.
- Password policies may also be enforced by training.

Example: A Good Password Policy

OGC follows a strict password policy. Employees are instructed to choose passwords that use a minimum of eight characters with a combination of numbers, upper and lowercase letters, and special characters such as punctuation. Employees are prompted by the system to change their passwords every month. This has helped enhance the security of company data.

The Shadow Password File

The *shadow password file* is a highly protected file that is used for storing each user's encrypted password. Unlike other password files, the shadow password file is readable only by the root user. This file can be accessed only by those processes that run at the root level.

Memory Usage

Memory usage is the sum of all the programs in the memory of an operating system. It also includes cached data. When more processes begin, the memory available for cache is reduced. If a limit is exceeded, Linux swaps out virtual memory processes that are idle most of the time.

Ways to Improve User-Level Security

There are a number of ways to improve user-level security. The following table lists some of the ways to improve user-level security.

Option	How This Helps
Limit the number of users	Prevents unauthorized users from accessing the system.
Limit the number of user logins	Specifies the maximum number of sessions a user can log in simultaneously.
Limit user accounts	Specifies the date when a user account should expire.
Limit hard disk and CPU memory usage	Sets quotas for individual users to limit memory usage on storage devices and the CPU so that the system performance is not affected.
Limit processes	Limits the number of simultaneous processes that a user can run so that the system performance is not affected.

How to Secure User Accounts

Procedure Reference: Execute Commands as a Superuser

To execute commands as a superuser:

1. Log in as a user other than root.
2. To run the command as the superuser, enter `sudo {command which needs root access}`.

3. Enter the password of the superuser or the user.
4. Observe that the command has been executed.

Procedure Reference: Implement Shadowed Passwords

To implement a shadowed password:

1. Log in as root in the CLI.
2. Implement shadowed passwords.
 - To implement a shadowed password for a user, enter `pwconv`.
 - To implement a shadowed password for a group, enter `grpconv`.
3. To verify that a shadow file has been created, enter `/etc/shadow`.

The `pwconv` and `pwunconv` Commands

The `pwconv` command removes the passwords created using the `passwd` command from the `/etc/passwd` file and creates a shadow password in the `/etc/shadow` file. This process can be reversed using the `pwunconv` command.

The `grpconv` and `grpunconv` Commands

The `grpconv` command removes the passwords created using the `passwd` command from the `/etc/group` file and creates a shadow password in the `/etc/gshadow` file. This process can be reversed using the `grpunconv` command.

Procedure Reference: Limit User Logins

To limit the number of user logins:

1. Log in as root in the CLI.
2. Enter `vi /etc/security/limits.conf`.
3. To limit the user logins, type *Username - maxlogins Number of logins*.
4. Save and close the file.

Number of Logins

You can specify the maximum number of sessions a user can log in simultaneously. For example, if you specify *Username - maxlogins 4*, it means that the user will be able to log in and run four different sessions simultaneously. If *Username* is replaced by `*`, it means that a maximum of four logins will be permitted simultaneously for all the users.

Limiting User Account

You can limit a user account by specifying its expiry date using the `usermod` command. For example, `usermod -e {yyyy-mm-dd} {login name}`.

The `ulimit` Utility

The `ulimit` utility sets or gets the file-size writing limit of files written by the shell and its descendants (files of any size may be read). Only a process with appropriate privileges can increase the limit. Limits are categorized as either soft or hard. With the `ulimit` command, you can change your soft limits, up to the maximum set by the hard limits. You must have root user authority to change resource hard limits. The table lists the `ulimit` command options.

If You Need To	Use This <code>ulimit</code> Command Option
List all of the current resource limits.	<code>-a</code>
Specify the size of core dumps, in number of 512-byte blocks.	<code>-c</code>
Specify the size of the data area, in number of K bytes.	<code>-d</code>
Specify that the hard limit for the given resource is set.	<code>-H</code>
Set the maximum size of files created by the shell.	<code>-f</code>
Specify the size of physical memory, in number of K bytes.	<code>-m</code>
Specify the maximum number of processes available to a single user.	<code>-u</code>

Procedure Reference: Disable Root Access for Telnet and FTP Services

To disable root access for Telnet and FTP services:

1. Log in as root.
2. Disable root access for the Telnet service.
 - a. Open the `/etc/securetty` file in any editor.
 - b. Remove the entries `tty0–tty9`.
 - c. Save the file.
 - d. If necessary, restart the Telnet service.
3. Disable root access for the FTP service.
 - a. Open the `/etc/vsftpd/ftpusers` file in any editor.
 - b. Remove the root entry.
 - c. Save the file.
 - d. If necessary, restart the vsftp service.

ACTIVITY 14-2

Resetting a Password

Before You Begin:

- 1. On srvA, you have logged in as root in the CLI.
- 2. The first terminal is displayed. Log out of the root user account.

Scenario:

You have administrative access to your Linux system. Your colleague, Eric, has forgotten the password to log in to his system, and you have been asked to help him.

What You Do	How You Do It
1. Switch to the root user account.	<ul style="list-style-type: none">a. Log in as jsmith.b. To switch to the root user account, enter su - rootc. Enter p@ssw0rdd. To view your user name, enter whoamie. Observe that you are logged in as the root user.
2. Change the password for Eric.	<ul style="list-style-type: none">a. To change the password of Eric, enter passwd ericb. To reset the password, enter myp@\$\$w0rd1c. To confirm the password, enter myp@\$\$w0rd1d. Observe that the password is reset. To exit the root user account, enter exit

3. Check whether the password is changed and log out of the system.
 - a. To switch to the **eric** user account, enter **su eric**
 - b. To log in with the old password, at the **Password** prompt, enter **myp@\$w0rd**
 - c. Observe that the login fails because the password is incorrect. To switch to the **eric** user account, enter **su eric**
 - d. To log in with the new password, at the **Password** prompt, enter **myp@\$w0rd1**
 - e. Observe that the login is successful. To exit the current user account, enter **exit**
 - f. Observe that you have switched back to the **jsmith** user account. To log out of the **jsmith** user account, enter **logout**
-

ACTIVITY 14-3

Securing User Accounts

Before You Begin:

1. On srvA, the first terminal of the CLI is displayed.
2. Log in as root.
3. At the command line, change the password of Eric to *myp@\$w0rd*.
4. Copy */etc/securetty* to */etc/securetty.bak*.
5. Copy */etc/vsftpd/ftpusers* to */etc/vsftpd/ftpusers.bak*.
6. Start the vsftpd service. Set the vsftpd service to automatically start at system startup.
7. Clear the terminal.

Scenario:

While researching ways to secure Linux systems, you come across a few articles stating that the root user should not have access to certain remote services to protect the security of the systems. Your manager wants you to secure the local user accounts on the Linux server. You decide to implement the necessary security features to prevent the root login from being used for Telnet and FTP services, to protect it from misuse.

LESSON 14

What You Do	How You Do It
1. Disable root access for the Telnet service.	<ol style="list-style-type: none">To open the file, enter vi /etc/securettyLocate "tty1" and delete the line.To delete the tty entries from tty2 to tty11, press D two times.To save and close the file, enter :wq
2. Access the Telnet service as the root user.	<ol style="list-style-type: none">Switch to srvB.To access the Telnet service, enter telnet 192.168.0.2Enter root as the user name.Enter p@ssw0rd as the password.Observe that the system displays "Login incorrect" because access is denied for the root user.To continue, press Ctrl+J.To return to the command prompt, enter quitTo clear the terminal screen, enter clear
3. Delete root access for the vsftpd service.	<ol style="list-style-type: none">Switch to srvA.To open the file, enter vi /etc/vsftpd/ftpusersLocate "root" and delete the line.To save and close the file, enter :wq

4. Access the ftp service as the root user.
 - a. Switch to `srvB`.
 - b. To access the ftp service, enter `ftp 192.168.0.2`
 - c. Enter `root` as the user name.
 - d. Observe that access is denied for the root user.
 - e. To return to the command prompt, enter `quit`
 - f. To clear the terminal screen, enter `clear`
-

TOPIC C

Enable Firewall Functionality

In the last topic, you secured user accounts as a level of security defense on your network. Now, you will look at packet filtering to provide firewall functionality to routers, gateways, and Linux servers and workstations. In this topic, you will implement iptables to provide firewall functionality by packet filtering.

When dealing with data navigating through your network, you will want to implement additional filtering. Understanding iptables will enable you to provide firewall functionalities by packet filtering to secure a Linux system. As a Linux administrator, you will need to provide a secure network and continuity of services, especially on large networks.

Firewalls

Definition:

A *firewall* is a software program or a hardware device that protects a system or a network from unauthorized access by blocking unsolicited traffic. A firewall allows incoming or outgoing traffic that is specifically permitted by an administrator. It also allows incoming traffic that is sent in response to requests from internal hosts. Firewalls often provide logging features and alarms that track security problems and report them to the administrator. Firewalls use packet filtering and proxy servers to implement security on a network.

Example:

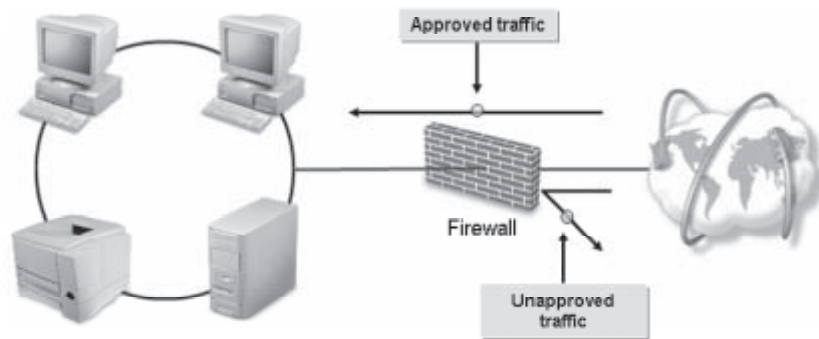


Figure 14-13: Firewall protects a network by filtering incoming and outgoing traffic.

Software Firewalls

The word “firewall” is generally used to refer to software-based firewalls. Software firewalls can be useful for small home offices and businesses. The firewall provides many features that can be configured to suit various computing needs. Some features include:

- Enabling or disabling port security on certain ports.
- Filtering inbound and outbound communication. A user can set up rules or exceptions in the firewall settings to limit access to the web.
- Reporting and logging activity.
- Protecting systems from malware and spyware.
- Blocking pop-up messages.
- Assigning, forwarding, and triggering ports.

Hardware Firewalls

A hardware firewall is a hardware device, either stand-alone or built into most routers, that protects computers on a private network from unauthorized traffic. They are placed between the private network and the public network to manage inbound and outbound traffic and network access.

Firewall Positioning

A firewall can be positioned logically between the internal network and the external world. In addition, it can be positioned between internal corporate networks and on individual servers. It is recommended to configure the firewall to either deny or grant access, based on the rules assigned by the security administrator.

Packet Filtering

Packet filtering is a process of passing or blocking incoming and outgoing packets after inspecting each packet for user-defined content, such as an IP address. It was the first type of firewall that was used to protect networks by reading packet headers. Packet filtering was limited by the fact that it was designed to look only at packet header information. *Netfilter* is a framework that implements packet filtering in Linux, to manage firewalls and secure data. It

contains a number of modules that inspect packet headers and filter packets with improper headers. The packets pass through various stages before they are sent to their destination. The packets are filtered at specific points and the filtered packets are sent to the next stage. Netfilter activities can be configured based on user requirements.

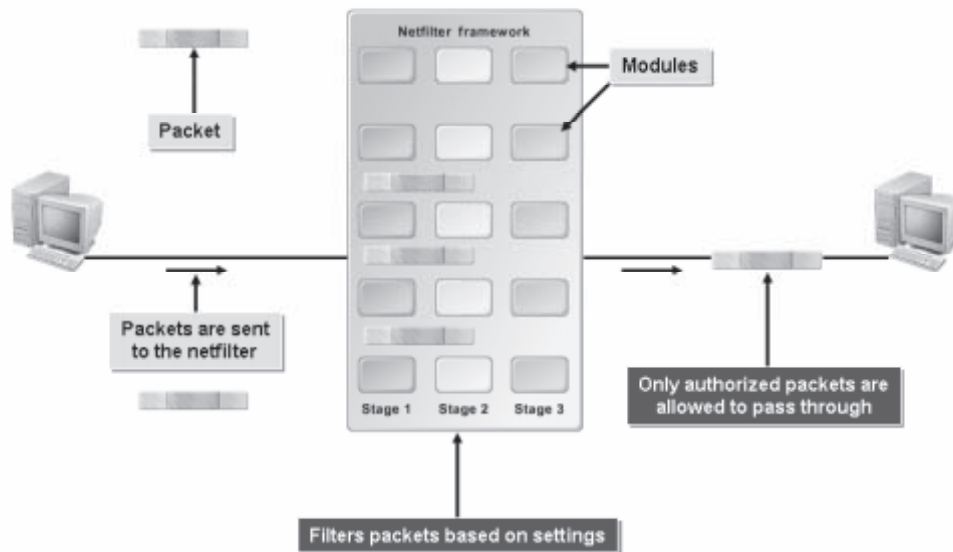


Figure 14-14: The working of the netfilter framework.

Proxy Server Implementation

A proxy server, also known as an application gateway, is a much more secure and flexible firewall solution than a pure packet filter. The proxy software can be configured to intercept network traffic. The proxy recognizes the request and sends the request to the server. In this way, the internal client never connects directly to the external server; thus, the proxy functions as the intermediary, communicating to both the client and the server. The major advantage is that the proxy software can permit or deny traffic based on the actual data in the packet, and not simply the header.

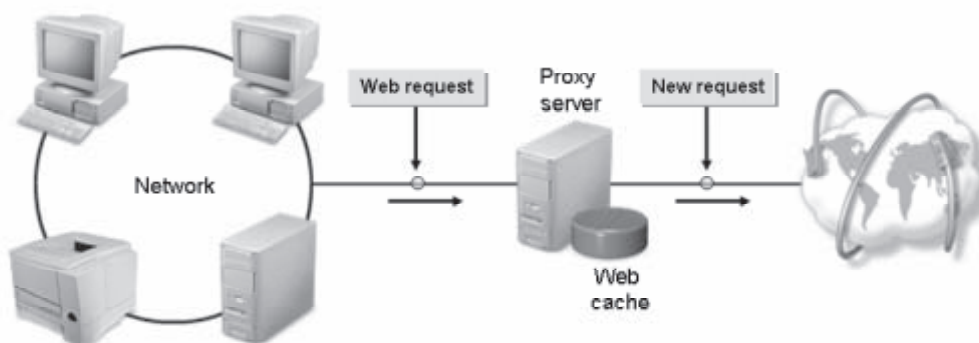


Figure 14-15: The functioning of a proxy server on a network.

The iptables Program

Definition:

The *iptables* program is a firewall program in Linux that provides protection to the internal network. This program uses rule sets, called *chains*, to implement *IP filtering*. Filter, nat, and mangle are the three iptables.

Example:

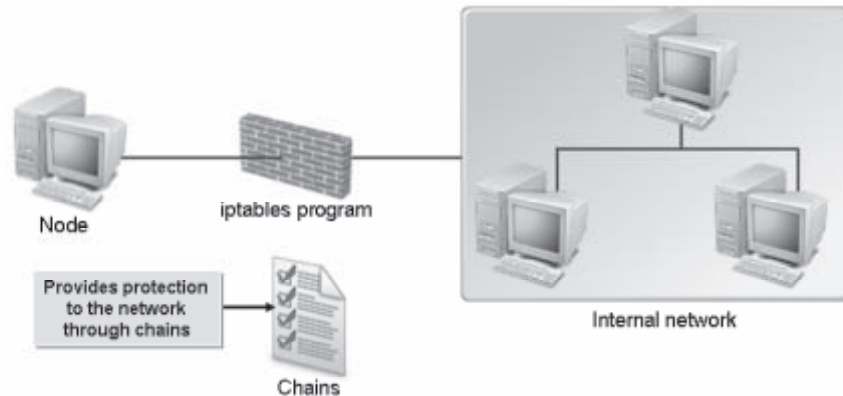


Figure 14-16: Protecting a network through chains defined using the iptables program.

Syntax

The syntax of the iptables program is `iptables [-t table] {commands} {chain/rule specification} [options/parameters]`.

The ipchains Program

The *ipchains* program is a Linux tool for managing packet filtering on a Linux server. Support for ipchains is compiled directly into the Linux kernel, where the ipchains tool inserts and deletes rules from iptables. These rules define whether packets are permitted or denied from being sent or received by a Linux system.



```

root@localhost:~
File Edit View Terminal Tabs Help
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
[root@localhost ~]#

```

Figure 14-17: A list of all the rules in the ipchains.

iptables and ipchains

One of the differences between ipchains and iptables is that iptables can be configured to be a stateful packet filter. With an iptable, the headers within a packet are examined against a known set of rules (the chain) in sequence. If the packet matches a rule, a decision is made for that packet based on what is specified (the target). If a match is not found, then the packet is examined against the next rule in the sequence. This continues until all the rules are exhausted. At this point, iptables look to ipchains to make the default policy decision.

Each iptable contains specific chains. The filter table contains the INPUT, OUTPUT, and FORWARD chains. The nat table contains the PREROUTING, POSTROUTING, and OUTPUT chains, and is used on networks where only outgoing packets have to be filtered. The mangle table contains the INPUT, OUTPUT, FORWARD, PREROUTING, and POSTROUTING chains, and is used on large networks where both incoming and outgoing packets have to be filtered.

Syntax

To check your installation for ipchains, use the `rpm -q iptables` command.

Use of ipchains

ipchains are used to block access to privileged ports of a Linux server. By blocking access to all incoming traffic, an administrator can prevent network access to a Linux workstation connected to a network.

How to Implement iptables

Procedure Reference: Configure iptables

To configure iptables:

1. Log in as root.
2. To start the iptables service, enter `service iptables start`.

- 3. To automatically start the iptables service at the system startup, enter `chkconfig iptables on`.
- 4. Manage the rules using iptables.
 - To add a rule, enter `iptables -A forward -p icmp -j ACCEPT`.
 - To remove a rule, enter `iptables -D forward -p icmp -j ACCEPT`.

ACTIVITY 14-4

Configuring iptables

Before You Begin:

- 1. Switch to srvA. You have logged in as root in the CLI.
- 2. At the command line, copy `/etc/securetty.bak` to `/etc/securetty`.
- 3. Overwrite the existing `securetty` file.
- 4. Copy `/etc/vsftpd/ftpusers.bak` to `/etc/vsftpd/ftpusers`.
- 5. Overwrite the existing `ftpusers` file.
- 6. Clear the terminal screen.
- 7. To log out, enter `exit` two times.
- 8. Log in as root.

Scenario:

Your need to implement a firewall on a Linux server and you decide to set up iptables on the Linux system. You need to check whether you are able to add and remove rules from the iptables.

What You Do	How You Do It
1. Start the iptables service.	<ul style="list-style-type: none">a. To start the iptables service, enter service iptables startb. To automatically start the iptables service at system startup, enter chkconfig iptables onc. To view the processes related to iptables, enter ps ax grep iptablesd. Verify that iptables is listed.

2. Add a rule to the iptable.
 - a. To add a new rule to accept TCP packets during the INPUT phase, enter


```
iptables -A INPUT -s 0/0 -i eth0 -d 192.168.0.1 -p TCP -j ACCEPT
```
 - b. To view the permissions for **INPUT**, **FORWARD**, and **OUTPUT** chains, enter


```
iptables -L | more
```
 - c. Verify that the new rule is added.
-
3. Drop a rule from the iptable.
 - a. To drop the rule related to TCP packets, enter


```
iptables -D INPUT -s 0/0 -i eth0 -d 192.168.0.1 -p TCP -j ACCEPT
```
 - b. To view the permissions for **INPUT**, **FORWARD**, and **OUTPUT** chains, enter


```
iptables -L | more
```
 - c. Verify that the rule is removed and clear the terminal screen.
-

TOPIC D

Implement Security Auditing

In the previous topic, you implemented iptables to provide firewall functionality on a Linux system by packet filtering. You will need to set up auditing for files and authentication in order to identify and trace possible security breaches. In this topic, you will implement security auditing.

A network may contain confidential data to which only selected people have access. This data may include financial reports, budgetary information, or personnel reviews. It is your responsibility to monitor the permissions and security levels on this data, so wouldn't you like to know if intruders are attempting to access data for which they do not have proper permission? When you implement security auditing, you can attain instant access to detect and record security-related events on your network.

How to Implement Security Auditing

Procedure Reference: Implement Security Auditing

To implement security auditing:

1. Set iptables to send possible intrusions to the log files by using the `iptables` command.

- 2. To save the iptables rule, enter the `service iptables save` command.
- 3. Direct the output from the iptables output to the `/var/log/iptables` file.

ACTIVITY 14-5

Implementing Security Auditing


Before You Begin:

- 1. On srvA, you have logged in as root in the CLI.
- 2. The first CLI terminal is displayed.
- 3. To navigate to the root directory, enter `cd /root`.
- 4. To clear the terminal screen, enter `clear`.

Scenario:

Your need to implement security auditing on your network. You decide to output the dropped packets from the iptables firewall to a log file where it can be reviewed for possible intrusion attempts.

What You Do	How You Do It
1. Set iptables to send possible intrusions to a log file.	<ul style="list-style-type: none">a. To create a chain named LOG_DROP, enter <code>iptables -N LOG_DROP</code>b. To append a new rule to the LOG_DROP chain, enter <code>iptables -A LOG_DROP -j LOG --log-tcp-options --log-level 3 --log-ip-options --log-prefix " [Dropped Packet] : "</code>c. To view the rules, enter <code>iptables -L</code>d. Observe that the LOG rule is listed in the rules of the LOG_DROP chain.e. To append a new rule to the LOG_DROP chain, enter <code>iptables -A LOG_DROP -j DROP</code>f. To view the rules, enter <code>iptables -L</code>g. Observe that the DROP rule is listed in the rules of the LOG_DROP chain. To save the iptables rules, enter <code>service iptables save</code>

2. Direct the iptables' output to /var/log/iptables.
 - a. To open the syslog.conf file, enter **vi /etc/syslog.conf**
 - b. To go to the end of the file, press **Shift+G**.
 - c. To switch to insert mode and move to a new line, press **O**.
 - d. To specify a description about directing iptable results to the log file, enter **#Log iptables results to iptables log**
 - e. To direct the results to the log file, type **kern.3** and press **Tab** and then type **/var/log/iptables**
 **kern** is used to log all kernel messages to the console.
 - f. To save and close the file, press **Esc** and enter **:wq**
 - g. To create the /var/log/iptables file, enter **touch /var/log/iptables**
 - h. To restart the syslog service, enter **service syslog restart**
-

TOPIC E

Describe the Intrusion Detection System

In the last topic, you implemented security auditing. To secure files that contain confidential data, you need to constantly monitor the network. In this topic, you will describe the Intrusion Detection System.

If your network is connected to the public network, chances are good that intruders may trace packets on the network and misuse services on your system. As a Linux administrator, you need to be aware of services on your network that will monitor any incoming and outgoing packets, and send an alert if any of the files or services have been corrupted or manipulated.

Network Monitoring Utilities

Various utilities are available for monitoring network devices and the systems connected to them.

Utility	Used To
nmap	Scan entire networks for various ports and the services running on them along with their status. The nmap utility can also be run as a GUI front end using the nmapfe command. This utility is primarily used to monitor remote network connections. There are a number of options for the nmap utility. These options help a user to get specific information about a network. The syntax of the nmap utility is <code>nmap [scan type] [options] {target specification}</code> .
tcpdump	Obtain packet information from a query string sent to the network interface. If the packet header matches the expression in the query, the packets are returned to the user. The syntax of the tcpdump utility is <code>tcpdump [options] {expression}</code> .
wireshark	Obtain packet information. It is a GUI-based utility. On running the wireshark command, the Wireshark Network Analyzer tool is displayed. Its functions are similar to the tcpdump utility.

The IDS

Definition:

The *Intrusion Detection System (IDS)* is a security sensor that protects portals, networks, and files from hackers. The IDS monitors system files, log files, and packets passed on the network. It also checks the network data stream for unauthorized signatures and attacks. IDS software can also analyze data and alert administrators to potential security problems. An IDS can comprise a variety of hardware sensors, intrusion detection software, and IDS management software.

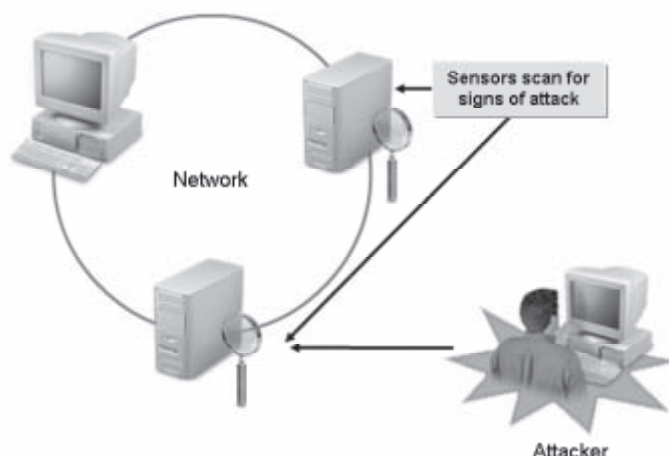


Figure 14-18: An IDS protecting a network from a hacker.

Example: Snort

Snort is an IDS that monitors each packet on the network. If a suspicious packet is detected, it passes an alert to the syslog file.

Passive and Active IDS

An IDS can be either passive or active. A *passive IDS* detects potential security breaches, logs the activity, and alerts security personnel. An *active IDS* does the same, and then takes the appropriate action to block a user from the suspicious activity. Some people consider the active IDS as a type of Intrusion Prevention System and not as a separate prevention system.

Tripwire

Definition:

Tripwire is an intrusion detection tool that compares the content of a file or directory with a database that contains the locations of the file or directory and the dates modified. It also monitors the attributes of the file such as the binary signature, size, or expected change of size. If the file has been changed, then the Tripwire tool passes an alert to the administrator by email.

Example:

Figure 14-19: Tripwire detects intrusion by comparing the content of a file and monitoring its attributes.

The Tripwire Database

The *Tripwire database* contains baselines, which are snapshots of files and directories noted at a specific time. When usage becomes abnormal, problems can be easily detected by comparing the latest files and directories with the earlier snapshots. After a Tripwire is installed and configured, the database should be initialized. To initialize the Tripwire database, execute the following command: `/usr/sbin/tripwire --init`. While initializing the database, Tripwire creates a collection of filesystem objects based on certain specifications mentioned in the policy file. An integrity check should be done after initializing the database. To view the entire database, enter the command `/usr/sbin/twprint -m d --print-dbfile | less`.

The tw.cfg File

The `tw.cfg` file is the Tripwire configuration file. Before generating the `tw.cfg` file, you can modify the configuration options in the `twcfg.txt` file to suit your requirements. The following table lists some of the configuration options.

Option	Used To
POLFILE	Modify the location of the policy file, <code>tw.pol</code> .
DBFILE	Modify the location of the database file, <code>[hostname].twd</code> .
REPORTFILE	Modify the location of the report file, <code>[hostname].[date].twr</code> .
SITEKEYFILE	Modify the location of the site key file.
LOCALKEYFILE	Modify the location of the local key file.
EDITOR	Specify the editor called by Tripwire when the database is updated.
MAILPROGRAM	Specify the mail program used by Tripwire.
MAILMETHOD	Specify the mail protocol used by Tripwire.



You cannot create the `tw.cfg` file if the Tripwire file locations are not properly specified in the `twcfg.txt` file.

Snort

Definition:

Snort is a network IDS that monitors network traffic. Snort monitors each packet on the network. If a suspicious packet is detected, it passes an alert to the syslog file and notifies the administrator through email or a pop-up window. It detects various network attack methods, including CGI attacks, denial-of-service, buffer overflow, and SMB probes.

Example:

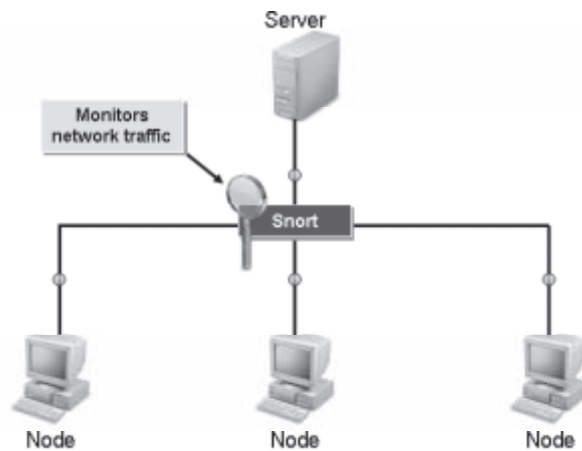


Figure 14-20: *Snort monitoring traffic on a network.*

Snort Options


Some frequently used `snort` command options are listed in the table.

Option	Used To
<code>-v</code>	Run Snort in verbose mode.
<code>-i {interface}</code>	Listen to packets on a specific interface.
<code>-l {directory}</code>	Specify the output logging directory.
<code>-n {number of packets}</code>	Specify the number of packets to be processed before exiting.
<code>-D</code>	Run Snort in daemon mode and log all messages in the <code>/var/log/snort/alert</code> directory.

Portsentry

Definition:

Portsentry is an IDS that detects and responds to port attacks. It is run as a daemon on TCP and UDP sockets to detect port scans on the system. If a port attack is detected, `portsentry` generates a log entry that contains the details of the hostname, the time of attack, the attacking host's IP address, and the TCP or the UDP port. It reports to the syslog daemon and alerts the administrator through email.

 Portsentry is generally used to drop the route to the scanning host. This prevents the attacking host from using any information it gained from the port scan.

Example:

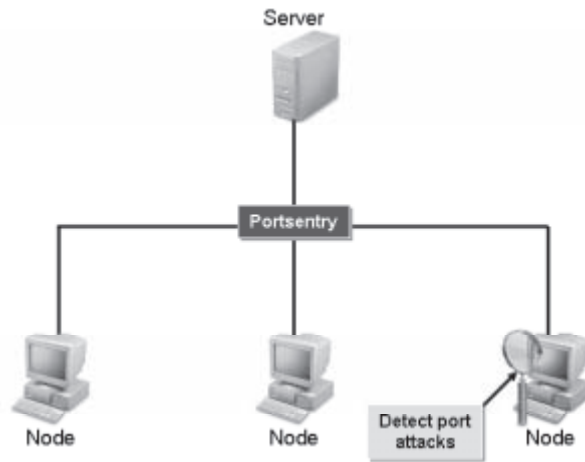


Figure 14-21: Portsentry detecting intrusion on a network.

Nessus

Definition:

Nessus is an IDS that audits the security of remote hosts and the services running on the network. Nessus performs vulnerability checks on the network and generates reports, listing all the security flaws and the possible ways to counter them. It consists of two parts, a server and a client. The server uses the `nessusd` daemon to maintain a vulnerability database for implementing security checks. The client uses this database and performs the security checks.

Example:

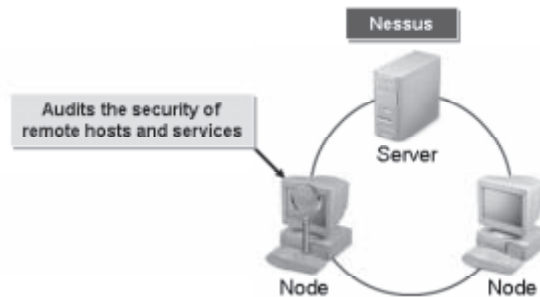


Figure 14-22: Portsentry auditing security on a network.

ACTIVITY 14-6

Describing Intrusion Detection Systems

Scenario:

You need to protect your system's configuration files. Any incorrect modification done to these files can corrupt your system because they contain critical information about your system. Therefore, you want to take special care to protect these files from being modified by intruders. You decide to study the methods that will allow you to detect intrusions.

-
1. **Which operations can be performed by the nmap command? Select all that apply.**
 - a) Scanning entire networks for various ports and the services running on them.
 - b) Returning packets to the user, if the packet header matches the expression in the query.
 - c) Obtaining packet information from a query string sent to the network interface.
 - d) Helping a user to get specific information about a network.
-
2. **Which of these can be a part of an IDS? Select all that apply.**
 - a) Hardware sensor
 - b) Intrusion detection software
 - c) Log files
 - d) IDS management software
-
3. **What does Tripwire do?**
 - a) Protects portals, networks, and files from hackers.
 - b) Compares the content of a file or directory with a database.
 - c) Obtains packet information from a query string sent to the network interface.
 - d) Monitors remote network connections.
-
4. **What is Snort?**
 - a) A detection tool that monitors the attributes of a file such as the binary signature, size, or expected change of size.
 - b) A software application that scans the ports for potential attacks.
 - c) A network IDS that monitors network traffic.
 - d) A tool that is used to crack system passwords.
-
5. **Which audits the security of remote hosts and services running on a network?**
 - a) Portsentry
 - b) Nessus
 - c) Tripwire
 - d) Snort
-

6. What does portsentry do when a port attack is detected?
-

Lesson 14 Follow-up

In this lesson, you examined various options available to secure a Linux system connected to a network. You configured encryption, secured user accounts, implemented iptables and security auditing, and detected intrusion. You will now be able to allow or restrict user access to network resources and safeguard your network by effectively protecting confidential data.

1. Which encryption method will you use to secure data? Why?
2. How will you detect intrusion on a network?

LESSON 15

Managing Hardware

Lesson Time*2 hour(s), 10 minutes*

In this lesson, you will manage hardware associated with Linux systems.

You will:

- Identify common hardware components and resources.
- Configure removable hardware.
- Configure disk quotas.

Introduction

In the last lesson, you configured various services and ensured the security of your network. While working with Linux, hardware-related issues will arise. In this lesson, you will manage hardware.

As a Linux administrator, you will need to upgrade hardware components regularly. By adding, removing, managing, and troubleshooting hardware, you can ensure the efficient working of your system.

This lesson covers all or part of the following CompTIA Linux+ Powered by LPI certification objectives:

- Topic A:
 - Objective 101.1, Objective 104.2
- Topic B:
 - Objective 101.1
- Topic C:
 - Objective 104.2, Objective 104.4

TOPIC A

Identify Common Hardware Components and Resources

There are various computer hardware and peripheral components available in the marketplace. However, not all are compatible with Linux. In this topic, you will identify common hardware components and resources for Linux.

Before you install any operating system, you need to have all your hardware and peripheral components in place. However, not all hardware are compatible with all systems. Having a thorough understanding of each component and how they work in a Linux system is critical for their successful installation.

Hardware Components

Basic hardware components of a Linux system include a Central Processing Unit (CPU) or Floating Point Unit (FPU), hard drives, memory, network adapters, and video cards. Additional components may include CD-ROM drives, sound cards, modems, USB devices, FireWire devices, PCMCIA/Cardbus cards, printers, or scanners.

Hardware Resources

Hardware resources, such as IRQs, DMA, memory addresses, and *Small Computer Systems Interface (SCSI)* IDs, can cause system configuration conflicts in a Linux system. To prevent such conflicts in your system, check the documentation before configuring the settings for a device resource. And when all devices are configured, do not keep changing their settings because it can be difficult; therefore, set the devices in such a way that they are not conflicting.

Types of SCSI

SCSI, pronounced as “skuzzy,” is a set of standards for connecting peripheral devices to a computer. It is a popular format for hard disks and CD-ROM drives. It has a fast transfer rate and can handle multiple devices. There are many SCSI types, each with their own specifications.

Type of SCSI	Bus Width and Maximum Throughput
SCSI-1	8 bits at 5 MB/sec
Wide SCSI	16 bits at 10 MB/sec
Wide Ultra SCSI	16 bits at 40 MB/sec
Fast SCSI	8 bits at 10 MB/sec
Fast Wide SCSI	16 bits at 20 MB/sec
Ultra SCSI	8 bits at 20 MB/sec
Ultra2 SCSI	8 bits at 40 MB/sec
Ultra3 SCSI	16 bits at 160 MB/sec
Ultra-320 SCSI	16 bits at 320 MB/sec
Ultra-640 SCSI	16 bits at 640 MB/sec

SCSI IDs

Each SCSI device has a unique SCSI ID, also known as a SCSI address, assigned to it so that the host adapter will be able to identify the device it is communicating with. The lowest SCSI ID is 0 and the highest is 7 or 15; 0 to 7 for narrow SCSI and 0 to 15 for wide SCSI. Priority is given based on the drive ID, 7 being the highest priority.

Normally, the Host Bus Adapter (HBA), which provides the interface between the system and SCSI, is assigned the ID of 7. Slower devices should have higher-priority IDs so that faster devices do not monopolize the bus. So, the primary hard drive should be assigned a lower number and a slow device, such as a tape drive, should be assigned a higher ID number. Priority for narrow SCSI is 7, 6, 5, 4, 3, 2, 1, 0; for wide SCSI, it is 7, 6, 5, 4, 3, 2, 1, 0, 15, 14, 13, 12, 11, 10, 9, 8. SCSI IDs are set using jumpers or DIP switches on the SCSI device.

IRQ Device Description

Check the IRQ address for non-plug-and-play devices to ensure that there are no conflicts. The following table shows IRQ and I/O addresses for floppy drives, printer ports, and COM ports.

Device	IRQ	I/O Address
fd0 (floppy disk drive 1)	6	3f0–3f7
fd1 (floppy disk drive 2)	6	3f0–3f7
fd2 (floppy disk drive 3)	10	370–377
fd3 (floppy disk drive 4)	10	370–377
lp0 (LPT 1)	7	378–37f
lp1 (LPT2)	5	278–27f

Device	IRQ	I/O Address
ttyS0 (COM 1)	4	3f8
ttyS1 (COM 2)	3	2f8
ttyS2 (COM 3)	4	3e8
ttyS3 (COM 4)	3	2e8

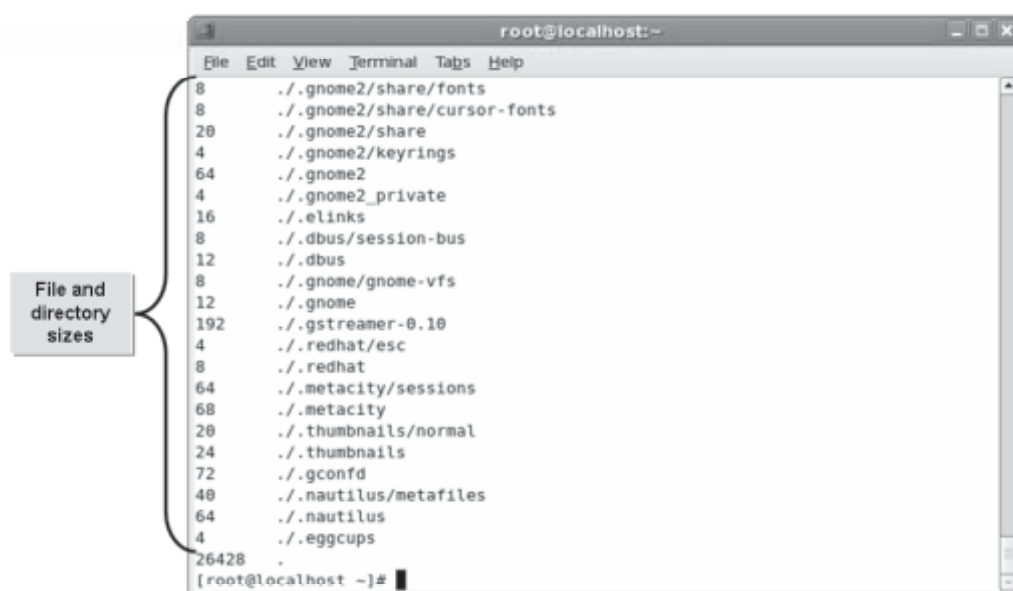
Disk Space Tracking

The *df* and *du* commands facilitate disk space tracking. The disk free (*df*) command enables you to view the free disk space, filesystem, total size, disk space used, percentage value of space, and mount point. The disk usage (*du*) command displays how a disk is used, including the size of directory trees and files within. It also enables you to track space hogs, which are directories and files that consume large amounts of space on the hard disk.

```

root@localhost:~
File Edit View Terminal Tabs Help
[root@localhost ~]# df
Filesystem              1K-blocks      Used Available Use% Mounted on
/dev/mapper/VolGroup00-LogVol00
18156292      5526428  11692700    33% /
/dev/sda1              101086        11969    83898    13% /boot
tmpfs                  517600           0    517600     0% /dev/shm
[root@localhost ~]#
  
```

Figure 15-1: The *df* command displaying free disk space.



```

root@localhost:~
File Edit View Terminal Tabs Help
8      ./gnome2/share/fonts
8      ./gnome2/share/cursor-fonts
20     ./gnome2/share
4      ./gnome2/keyrings
64     ./gnome2
4      ./gnome2_private
16     ./elinks
8      ./dbus/session-bus
12     ./dbus
8      ./gnome/gnome-vfs
12     ./gnome
192    ./gstreamer-0.10
4      ./redhat/esc
8      ./redhat
64     ./metacity/sessions
68     ./metacity
20     ./thumbnails/normal
24     ./thumbnails
72     ./gconfd
40     ./nautilus/metafiles
64     ./nautilus
4      ./eggccups
26428 .
[root@localhost ~]#

```

File and directory sizes

Figure 15-2: The `du` command displaying the size of directories and files on the disk.

How to Identify Common Hardware Components and Resources

Procedure Reference: Identify Hardware Components and Resources

To identify hardware components and resources:

1. Log in as root.
2. Switch to the `/proc` directory.
3. Document the hardware components for future reference.
 - To display CPU information, use the `cat cpuinfo` command.
 - To display device information, use the `cat devices` command.
 - To display partition information, use the `cat partitions` command.
 - To display current hard disk size and usage, use the `df -h` command.
 - To display current IRQ resources, use the `cat interrupts` command.

ACTIVITY 15-1

Determining Hardware Components and Resources

Before You Begin:

- 1. On srvA, you logged in as root.
- 2. The first terminal is displayed.

Scenario:

Jane wants all her team members to switch to Linux systems, to better align with other departments in the company. To finalize additional hardware requirements, she wants you to document the resources that the current Linux systems are using so that she can decide on her own team’s system requirements.

What You Do	How You Do It
1. Document the CPU information.	<ul style="list-style-type: none">a. To view details about the CPU, at the command line, enter cat /proc/cpuinfob. Document the model name, processing power (in MHz), and cache size.
2. Document the device information.	<ul style="list-style-type: none">a. To view the list of current character and block devices, enter cat /proc/devicesb. Document the current character and block devices.
3. Document the number of hard drive partitions and the current usage statistics.	<ul style="list-style-type: none">a. To view the list of partitions, enter cat /proc/partitionsb. Document the number of hard drive partitions.c. To view the amount of free space in each hard drive, enter df -hd. Document the details about the total hard drive size, the amount of space used, and the amount still available.

4. Document the IRQ resources.
 - a. To view the IRQ list for various devices, enter `cat /proc/interrupts`
 - b. Document the IRQs for each device listed.
 - c. Clear the terminal screen.
-

TOPIC B

Configure Removable Hardware

In the last topic, you examined hardware requirements for Linux systems. As a Linux administrator, you may need to add additional hardware devices or external peripherals to your system based on user requirements. In this topic, you will configure removable hardware.

Advancements in technology may require you to constantly upgrade the hardware configuration of your Linux system. Removable devices are a convenient and efficient way to upgrade your Linux system.

Removable Hardware

Linux systems allow you to utilize removable devices. Some of these devices are described in the following table.

Device	Example
Input	Keyboard, pointing device, joystick, scanner, webcam, digital tablet, and digital camera
Network	Modem and NIC
Output	Printer, sound card, and speakers
Storage	CD, DVD, tape drive, floppy disk, zip drive, flash drive, and hard drive

The PC Card

The PC Card is designed for use as a storage device, network card, and modem. Its standards and specifications are defined by the Personal Computer Memory Card International Association (PCMCIA). The PC Cards were formerly known as PCMCIA Cards.

The PCMCIA Organization

The PCMCIA organization is an alliance that promotes interchangeability and compatibility among portable computers. The alliance defines the standards for the PC Card.

Card and Socket Services

Card and socket services are loaded into the memory when a portable computer is booted. This software comes with the PC and its cards. These are two layers of software that detect and support a PC Card when inserted. They also manage hot-swapping and pass changes in events to higher level drivers written for specific cards.

Socket services interact with BIOS to identify the number of sockets available. It can be built into BIOS or added through software. When the system is turned on, it detects when a PC Card is inserted or removed. Socket services work with card services above it and communicate directly with the PC Card's controller chips.

Card services automatically assign system resources when socket services identify that a PC Card has been inserted. Card services manage system resources required by PC Cards such as IRQs, memory, and I/O addresses. This software management interface also works in conjunction with upper level software, such as hardware drivers, that may need to be loaded to work with the PC Card.

The cardmgr Utility

The cardmgr utility monitors PCMCIA sockets for card insertion and removal events. When a card is inserted, the utility looks up the card in a database of known cards. If the card is identified, appropriate device drivers are loaded and bound to the card. When the card is ejected, the card's drivers will be unloaded, if possible.

The `/var/run/stab` file, created by the cardmgr utility, contains identification and device driver information for PCMCIA cards. Device driver lines comprise a series of tab-separated fields. These fields are described in the following table.

Field	Description
1	Socket number
2	Device class (identifies which script in <code>/etc/pcmcia</code> is used to configure or shutdown the device)
3	Driver name
4	Used to number devices when a single card has several devices associated with the same driver
5	Device name
6	Major device number, if required
7	Minor device number, if required

Arbitrary Commands

Based on the contents of the PCMCIA Card configuration database, the cardmgr utility may also execute arbitrary commands when appropriate cards are either inserted or removed. All insertion and removal events, device driver loads and unloads, startup and shutdown commands, and warnings and errors are reported in the system log file. Current card and device information for each socket is recorded in the `/var/state/pcmcia/stab` or `/var/lib/pcmcia/stab` file.

Normally, when a card is identified, the `cardmgr` utility will send a beep to the console. A beep is also generated when a card is successfully configured. A beep of lower pitch is generated if either of these steps fails. Ejecting a card produces a single beep. When the `cardmgr` utility receives a `SIGHUP` signal, it will reload its configuration file. When the `cardmgr` utility receives a `SIGTERM` signal, it will shutdown all sockets that are not busy and then exit, but drivers for busy sockets will stay loaded. If the `PCMCIA_OPTS` environment variable is set, its contents will be parsed after the main card configuration file is read.

The `pcmcia` File

The `pcmcia` file stored in the `/etc/pcmcia/config` directory is a card configuration database. It is read at startup by the `cardmgr` utility. It defines the resources that are available for use by the card services, explains how to load and initialize device drivers, and describes specific PCMCIA cards.

Stab File Update

The stab file is updated by the `cardmgr` utility whenever a card is inserted or ejected and when the `cardmgr` utility receives a signal. The stab file will normally be created in either the `/var/state/pcmcia` or `/var/lib/pcmcia` files, but if neither directory is available, it will be found in the `/var/run` file.

The `pccardctl` Utility

The `pccardctl` utility, which has replaced the `cardctl` utility, is used for monitoring and controlling the state of PCMCIA sockets. If `pccardctl` is executed by the root user, all commands are available. If it is executed by a user with limited access rights, only the informational commands are accessible. The card control commands are listed in the following table.

Command	Description
<code>status</code>	Displays the current socket status flags.
<code>config</code>	Displays the socket configuration, including power settings, interrupt and I/O window settings, and configuration registers.
<code>ident</code>	Displays the card identification information, including product identification strings, manufacturer ID codes, and function codes.
<code>suspend</code>	Shuts down and then disables the power for a socket.
<code>resume</code>	Restores power to a socket and reconfigures it for use.
<code>eject</code>	Notifies all client drivers that the PC Card will be ejected and then cuts power to the socket.
<code>insert</code>	Notifies all client drivers that the PC Card has just been inserted.



If the command is to be applied to just one socket, the socket number should be specified; otherwise, all sockets will be affected.

Selecting PCMCIA Configuration Schemes

You can use the `cardctl` utility to select from among multiple PCMCIA configuration schemes. The current scheme name is passed to the device option scripts as part of the device address so that the scripts can use it to choose from among different setups.

The USB

The *Universal Serial Bus (USB)* is a hardware interface standard designed to provide connections for numerous peripherals. *USB devices* are peripheral devices that communicate with a host computer. Some common USB devices include flash drives, memory card readers, and digital cameras.

USB Standards

USB 2.0 is the most commonly implemented standard. It can communicate at a rate of up to 480 Mbps. The original USB 1.1 standard is still commonly found in devices and systems. It can communicate at a rate of up to 12 Mbps. A USB 2.0 device connected to a USB 1.1 hub or port will communicate at only USB 1.1 speeds, even though it may be capable of faster speeds. Generally, the operating system will inform you of this when you connect the device.

USB 3.0, also called SuperSpeed USB, is the latest USB standard released and features a maximum transfer rate of 5.0 Gbit/s. It is 10 times faster than the USB 2.0 standard, has enhanced power efficiency, and is backward compatible with USB-enabled devices currently in use.

USB cables have a maximum distance before performance suffers. To work around this, one or more hubs can be used to create a chain to reach the necessary cable length. USB 1.1 has a maximum cable length of 3 meters, while USB 2.0's maximum length is 5 meters. In each case, a maximum of five hubs can be used to extend the cable length.

USB Plug and Play Capabilities

USB devices also incorporate plug-and-play technology that allows devices to self-configure as soon as a connection is made.

Kernel Support

While using USB devices, make sure that you have a kernel that includes USB support. Limited USB support was added in kernel 2.2.18, but it's best to run the 2.4.0 test kernel and any applicable patches for the next kernel. Be diligent in keeping up to date with new versions, because they tend to change frequently.

USB in Linux

Linux treats USB devices like SCSI disks, registering the first device as `/dev/sda`, where "sda" means the first partition of the first device.

The Basic Architecture of the Layer Model of a USB Driver

The basic architecture of a USB driver consists of a host computer, an upper software layer, a host controller hardware layer, a physical bus, and one or more USB devices. The following table lists the components and their description.

Component	Description
<i>Host Computer</i>	Consists of two layers and controls data transfer to and from USB devices.
Upper Software Layer	Includes the USB device drivers.

Component	Description
<i>Host Controller Hardware Layer</i>	Converts data between the format used by the host computer and the physical format used by the USB. It is also known as the adapter layer.
<i>Physical Bus</i>	Consists of a set of USB cables that link the controller with the peripherals.
<i>USB Devices</i>	Peripheral devices that use the USB electrical and data format specifications to communicate with the host computer.

Host Controller Interface

Host Controller Interface (HCI) is an interface that instigates communication between an external device driver and the operating system of a PC. Enhanced Host Controller Interface (EHCI), Open Host Controller Interface (OHCI), and Universal Host Controller Interface (UHCI) are different standards grouped under HCI, which are collectively referred to as xHCI modules, where x being a variant is E or O or U depending on the characteristics of the modules installed.

FireWire

FireWire is an IEEE 1394-standard, high-speed serial bus, much like USB, which can run up to 30 times faster than USB. FireWire's higher bandwidth makes it ideal for devices such as digital video cameras and high-speed hard disk drives.

FireWire Cables

In FireWire cables, electrical contacts are inside the structure of an IEEE 1394 cable connector. This helps protect the user from electric shocks. These cables are easy and safe to use. Users can blindly insert them into the systems. Terminators are not required and manual IDs do not have to be set.

The 1394 Subsystem Core

The core of the 1394 subsystem is a module that manages high- and low-level drivers, handles transactions, and triggers events. Subsystem high-level drivers, or routines, register themselves with the IEEE 1394 module by calling the function `hpsb_register_highlevel`.

The Loopback Device

The loopback device in a Linux system allows you to access a file or a set of files as a block device. It allows you to mount filesystem images, such as ISO, CD images, and floppy disk images, on the hard disk. You can create a floppy disk or CD, complete with the filesystem and files, on your Linux filesystem without actually copying or burning it onto the media. A copy of the floppy or CD can be taken later. Loopback devices are also used for filesystem encryption.

How to Configure Removable Hardware

Procedure Reference: Configure USB Hardware

To configure USB hardware:

1. Verify that the kernel version of your system is 2.4 or above.
2. Verify that the `/proc/bus/usb` directory has been created.



The `/proc/bus/usb` directory contains subdirectories with information about the USB devices connected to the system.

3. Install the drivers for the device.
4. Plug in the device.

Procedure Reference: Configure PCMCIA Hardware

To configure PCMCIA hardware:

1. Check if the PCMCIA module is compiled in the kernel.
2. Verify that the `/etc/pcmcia/config.opts` file has been created.
3. Install any necessary drivers for the device.
4. Plug in the device.
5. Configure the device by using the `cardmgr` utility.

Procedure Reference: Activate the USB Support

To activate the USB support:

1. Ensure that a USB card has been installed in your system.
2. Log in as root in the CLI.
3. Enter `vi /etc/modprobe.conf`.
4. To load the USB card driver depending upon the USB driver during boot time, enter `alias usb-controller usb driver/xHCI driver`.
5. Save and close the file.
6. Reboot the system.
7. If necessary, verify that the USB support has been activated.
 - a. Log in as root.
 - b. Connect the USB devices.
 - c. To view the connected USB devices, enter `lsusb`.

DISCOVERY ACTIVITY 15-2

Discovering Removable Hardware

Scenario:

Your manager, Linda, is pleased with the ease of use and ultimate success of the Linux implementation. She would like to expand the use of Linux to business laptops and other desktops with removable devices. Check the use of removable hardware with Linux and report the results to your manager.

1. Which of these statements are true? Select all that apply.

- a) USB is an IEEE 1394-standard, high-speed serial bus.
 - b) A loopback device allows you to mount filesystem images, such as ISO, on the hard disk.
 - c) FireWire is ideal to connect a digital video camera to a system.
 - d) The PCMCIA was formerly known as the PC Card.
 - e) The cardmgr utility is used to monitor and control the state of PCMCIA sockets.
-

2. Which is the earliest kernel that supported USB?

- a) 2.2.18
 - b) 2.4.16
 - c) 2.6.22
 - d) 2.2.13
-

3. True or False? USB device information is located in the /proc/usb directory.

- ☐ True
 - ☐ False
-
-

TOPIC C

Configure Disk Quotas

In the last topic, you identified and configured removable hardware. One such common removable hardware device is an external storage device, which can be used to access stored files, backup built-in storage devices, or store regularly used files. External storage devices are helpful when the hard disk space is not sufficient to store what a user requires. One way to manage this is to ensure that all users have access to sufficient disk space for storing individual files that they need to access regularly, but not so much space for files that they will never use again. In this topic, you will configure disk quotas.

One of the tasks that a system administrator must undertake is limiting disk space usage. Users may need to store files and data in a common location. By configuring disk quotas, you can ensure that all users have adequate storage space in that common location.

Disk Quotas

Definition:

A *disk quota* is the disk space that is allotted to a user for file storage on a computer. Disk quotas need to be configured for each user. Every filesystem for which a disk quota has been implemented will have a default grace period of seven days. This means that when a user has reached the soft limit, the grace limit feature gets activated. The soft limit is the quota value beyond which disk space usage is allowed only during the grace period. Once the grace period expires, the soft limit will be enforced as the hard limit, a maximum number will be set on disk usage and users cannot exceed this limit.

Example:

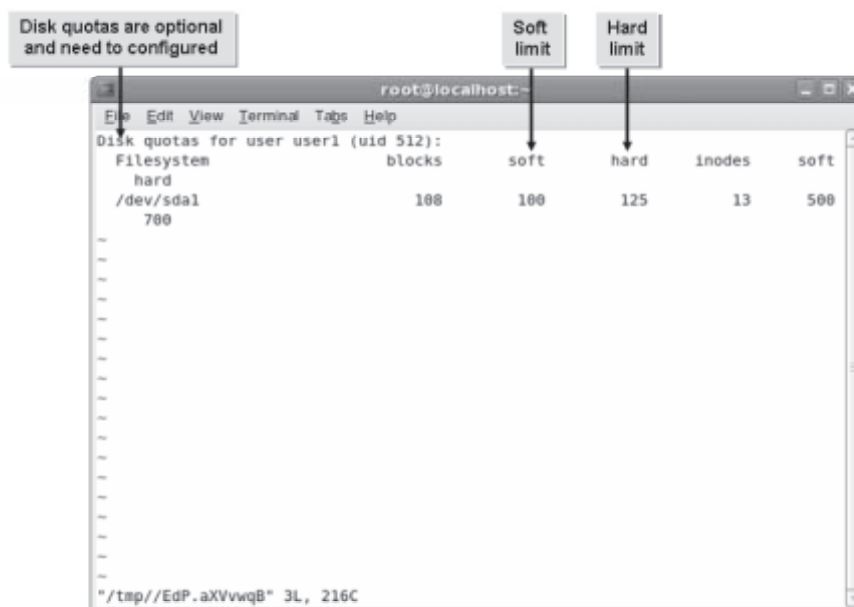



Figure 15-3: The disk quota for a user.

Quota Management Commands

Quota management is the effective allotment and monitoring of quotas for all users. Linux has various commands that help ease the job of quota management for the system administrator.

 Quotas should be assigned in such a way that users are able to maximize the utilization of disk resources without data overflow.

Command	Used To
<code>edquota -u {user name}</code>	Edit quotas for a specific user.
<code>edquota -g {group name}</code>	Edit quotas for a specific group.
<code>setquota -u {user name}</code>	Set quotas for a specific user.
<code>setquota -g {group name}</code>	Set quotas for a specific group.

Quota Reports

Quota reports are created by the system to view the usage of disk space by each user. These reports enable the system administrator to check which user is taking up maximum disk space. There are two types of quota reports: user quota reports and group quota reports.

Contents of a Quota Report

A quota report contains the following details:

- The name of the user.
- The total number of blocks (in kilobytes) that have been utilized by the user on a partition.
- The *soft limit*, which is the maximum amount of disk usage that a quota user has on a partition.
- The *hard limit*, which is the absolute limit on disk usage that a quota user has on a partition.
- The *grace period*, which is the time limit before the soft limit is enforced for a filesystem with quota enabled.
- The total number of inodes that have been used on a partition by a user.
- The soft limits on inodes.
- The hard limits on inodes.

The quotacheck Command

The `quotacheck` command examines filesystems for which you enabled quotas, builds a table of current disk usage, and updates the `aquota.user` file. The `quotacheck` command has various options.

Option	Used To
<code>-g</code>	Check group quotas.

Option	Used To
-u	Check user quotas.
-a	Check all mounted non-NFS filesystems specified in the <code>/etc/mtab</code> file.
-b	Back up the quota file before writing new data.
-c	Perform a new scan and save it to the disk.

Quota Reports Generation Commands

A number of commands are available for the generation of effective quota reports.

Command	Enables You To
<code>repquota -a</code>	Display the reports for all filesystems indicated as read-write with quotas in the <code>/etc/mtab</code> file.
<code>repquota -u {user name}</code>	Display the quota report for a particular user.
<code>quota -uv {user name}</code>	Display the quota report for a particular user with verbose output.
<code>warnquota -u</code>	Check if users are not exceeding the allotted quota limit.
<code>warnquota -g</code>	Check if groups are not exceeding the allotted quota limit. In case of quota being exceeded a mail is sent to the user mentioned in the <code>/etc/quotagrpadmins</code> file.

How to Configure Disk Quotas

Procedure Reference: Set Disk Quota for a Filesystem

To set disk quota for a filesystem:

1. Log in as root in the CLI.
2. Specify user quota for the partition you want to allocate to users.
 - a. Enter `vi /etc/fstab`.
 - b. In the fourth field of the partition entry, change the default values.
 - To define user quota for the specified partition, change defaults to `defaults,usrquota`.
 - To define group quota for the specified partition, change defaults to `defaults,grpquota`.
 - To define user and group quota for the specified partition, change defaults to `defaults,usrquota,grpquota`.
 - c. Save and close the file.
3. To remount the partition, enter `mount -o remount {mount point}`.
4. To scan for the disk usage and create a quota file, enter `quotacheck -c {mount point of the partition}`.

Procedure Reference: Manage Quota Service on a System

To manage quota service on a system:

1. Log in as root in the CLI.
2. Manage the quota service on the system.
 - To turn on the quota, enter `quotaon [options] {mount point}`.
 - To turn off the quota, enter `quotaoff [options] {mount point}`.

Procedure Reference: Set Quota for Users

To set quotas for users:

1. Log in as root in the CLI.
2. Set quotas for users.
 - To set user quota, use the `edquota` command.
 - a. Enter `edquota [options] {user or group name}`.
 - b. Specify the soft and hard limits for blocks and inodes.
 - c. Save and close the file.
 - To set quotas for users using the `setquota` command, enter `setquota [options] {user or group name} {soft block limit} {hard block limit} {soft inode} {hard inode} [options] /dev/{device name}{partition number}`.

Procedure Reference: View Quota Reports

To view the quota report:

1. Log in as root in the CLI.
2. View the quota report.
 - To display the quota report for the user or group, enter `quota [options] [user or group name]`.
 - To display the quota report for the specified mount point, enter `repquota [options] {mount point}`.
 - To send the quota report as a mail message to the user as configured in `/etc/warnquota.conf`, enter `warnquota [options]`

ACTIVITY 15-3

Configuring User Quota

Before You Begin:

1. On *srvA*, you have logged in as root in the CLI.
2. On the terminal, create a new user account, *user2*
3. Set *myp@\$w0rd* as the password for the *user2* account.
4. If necessary, enter *quotaon -a* to enable disk quota.
5. Clear the terminal screen.

Scenario:

Your company has a common server that is used by all employees to store and share files internally. You have received complaints from users on the network about low disk space on the common server because some employees have excessive amounts of data on it. You decide to assign disk quotas to limit disk space usage for users according to the following details:

Space to be allocated to *user1* and *user2*:

- Block soft limit=100
- Block hard limit=125
- Inode soft limit=500
- Inode hard limit=700

The quota has to be set for *user1* and *user2*.

What You Do	How You Do It
1. Configure the user quota for the partition /.	<ol style="list-style-type: none">To open the <code>/etc/fstab</code> file, on the terminal, enter vi /etc/fstabTo switch to insert mode, press I.To set user quota for the <code>/</code> partition, on the line LABEL=/ / ext3 defaults 1 1, after the word "defaults," add ,usrquotaTo switch to command mode, press Esc.Save and close the file.To restart the system, enter rebootLog in as root in the GUI.To display the terminal window, choose Applications→Accessories→Terminal.To scan for the disk usage and to create a quota file, enter quotacheck -cum /

LESSON 15

2. Specify the disk space usage.
 - a. To edit the user1 quota, enter **edquota -u user1**
 - b. To switch to insert mode, press **I**.
 - c. Specify the hard and soft limit values for user1 as given in the scenario.
 - d. Press **Esc**.
 - e. Save and close the file.
 - f. Specify disk space usage for user2 and save the file by following steps from (a) to (e).
 - g. To clear the terminal window, enter **clear**
 - h. To apply the changes, enter **quotaon -u /**
 - i. To clear the terminal window, enter **clear**
-

Lesson 15 Follow-up

In this lesson, you managed hardware associated with Linux systems. You will now be able to safely and efficiently replace, upgrade, manage, and troubleshoot any piece of hardware in Linux systems.

1. What are the benefits of implementing RAID on a network?
2. What are the advantages of assigning disk quotas? Why?

LESSON 16

Troubleshooting Linux Systems

Lesson Time

1 hour(s)

In this lesson, you will troubleshoot Linux system issues.

You will:

- Use the Linux rescue environment for troubleshooting the Linux system issues.
- Troubleshoot hardware issues.
- Troubleshoot network connection and security issues.

Introduction

While working with a Linux operating system, users may experience unexpected technical issues. To provide uninterrupted services to the users, you need to be able to solve the problems that arise while functioning. In this lesson, you will troubleshoot Linux-related issues.

As an administrator managing multiple systems on a network, you would have installed various services and packages required by users. However, when several users start using the systems, there may be instances when the applications and services do not function as desired. As the administrator, you will be expected to determine and resolve the problems.

This lesson covers all or part of the following CompTIA Linux+ Powered by LPI certification objectives:

- Topic A:
 - Objective 101.2, Objective 102.1, Objective 110.1
- Topic B:
 - Objective 101.2, Objective 106.1, Objective 108.4
- Topic C:
 - Objective 109.3

TOPIC A

Troubleshoot System-Based Issues

Previously, you managed hardware devices that help make up an entire Linux system. While Linux is inherently a stable system, it does need troubleshooting and servicing from time to time. While working with Linux, you may experience issues that may prevent you from using the system or its services. In this topic, you will troubleshoot system-based issues to help recover the Linux system.

As an administrator managing multiple systems on a network, you will eventually experience a wide variety of issues with the Linux operating system. Without proper identification and analysis, finding a solution will not only be time consuming, but also cumbersome. Therefore, you must familiarize yourself with the procedures required to identify these issues and solve them efficiently.

Troubleshooting Strategies

A troubleshooting strategy is a plan of action for identifying the causes and resolving the effects of a system-related issue. Various guidelines have to be considered while troubleshooting.

Guideline	Description
Analyze the problem	Before attempting to troubleshoot an issue, try to identify the problem through its symptoms, such as error messages, and other available information such as log files and configuration files. Also, check if the relevant services are working properly.
Back up data	Before experimenting with issues in configuration files, log files, or any other important data, it is recommended to make a backup to avoid loss of information and further complication of the issues.
Eliminate possible causes	Observe whether the issue is related with the hardware, an application, a process, or any other service. Try to choose one or more symptoms and drill down to the root cause. Eliminating the root cause will rectify all the related issues.
Adopt fundamental problem-solving approaches	After identifying the underlying causes, try out the fundamental methods of resolving the issue before proceeding to complicated problem solving procedures.

A Basic Troubleshooting Model

Some companies developed troubleshooting processes that are systematic and logical. Following these guidelines will help you find and correct problems on your network quickly and efficiently. One troubleshooting model divides the troubleshooting process into four steps.

1. Gather basic information.
2. Develop a plan of action.
3. Execute the plan and isolate the problem.
4. Document the solution.

Troubleshooting can be a difficult process. It is not likely that anyone can develop a complete and accurate approach to troubleshooting, because troubleshooting is often done through intuitive guesses based on experience.

The Linux Rescue Environment

The *Linux rescue environment* is a stand-alone Linux program for troubleshooting a corrupt Linux installation. It serves as an external environment through which errors in the Linux system can be fixed without the help of the existing installation files. The rescue environment mounts the standard Linux system directories in the `/mnt/sysimage` directory. These directories are mounted either in read-write mode or read-only mode, depending on the kinds of issues.

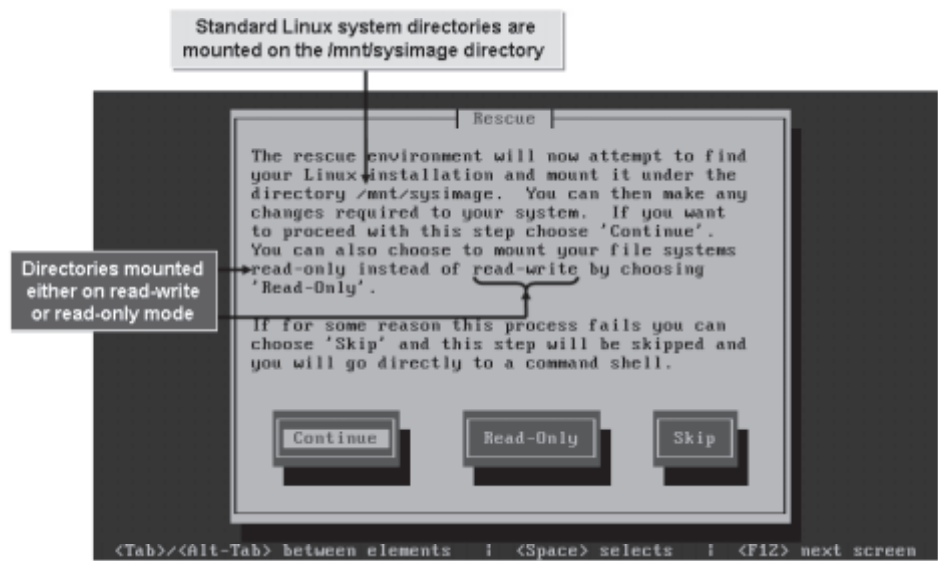


Figure 16-1: The rescue environment for troubleshooting Linux issues.

 In some cases, when system directories cannot be mounted on the /mnt/sysimage directory, the prompt will be available for troubleshooting.

chroot Mode

chroot mode shifts the /root directory to a different location for recovery. It is also known as jail mode because a user will not be able to access any other file or directory except this directory and its subdirectories.

Rescue Environment Utilities

A set of utilities is available in the rescue environment to troubleshoot different issues.

Category	Utility
Disk Maintenance Utilities	<ul style="list-style-type: none">• LVM utilities such as lvcreate, lvresize, and lvremove.• Software RAID utility such as mdadm.• Disk partitioning and swap utilities such as fdisk, sfdisk, mount, umount, and mkswap.• Filesystem utilities such as mkfs, tune2fs, fsck, and e2fsck.
Networking Utilities	<ul style="list-style-type: none">• Network debugging utilities such as ifconfig, route, dig, netstat, traceroute, host, and hostname.• Network connectivity utilities such as ssh, ftp, and scp.

Category	Utility
Other Utilities	<ul style="list-style-type: none"> • Shell commands such as <code>chroot</code> and <code>bash</code>. • Process management tools such as <code>ps</code> and <code>kill</code>. • Editors such as <code>vi</code> and <code>nano</code>. • File management commands such as <code>cd</code>, <code>ls</code>, <code>cp</code>, <code>rm</code>, and <code>mv</code>. • Kernel management utility such as <code>sysctl</code>. • Package management tools such as <code>rpm</code> and <code>yum</code>. • Archiving and compression utilities such as <code>tar</code> and <code>gzip</code>.

Environment Configuration Problems

Configuration problems could prevent a user from logging in to a system and accessing the services provided by the server. Other problems could also be caused due to system variables or due to user and group accounts. The symptoms, causes, and solutions for common configuration problems are provided in the following table.

Symptom	Cause and Solution
The user is unable to create a user or a group account.	<p>Cause: The user does not have admin privileges, or the system is unable to allocate memory to the user account due to insufficient memory.</p> <p>Solution: Check whether the required privileges are granted to the user. Also, check for free space in the memory that can be allocated to the user account.</p>
The user is unable to log in.	<p>Cause: The settings in the user account or the group account could be wrong.</p> <p>Solution: Check the user or group account settings, including the permission to log in to the system, the shell, and the path of the home directory.</p>
The user is unable to access files and directories.	<p>Cause: The required permission is not granted to the user.</p> <p>Solution: Check the user or group quota and the privileges granted to the user.</p>
The user is unable to execute basic commands or applications.	<p>Cause: The environmental variable is not properly set.</p> <p>Solution: Check the environmental variables and the library files of the application.</p>
The scheduled jobs are not executed.	<p>Cause: The <code>crond</code> daemon has not started or stopped due to the invalid configuration.</p> <p>Solution: Check whether the <code>crond</code> daemon is running. Otherwise, check whether the configuration set in the crontab file is correct.</p>

Symptom	Cause and Solution
The user is unable to switch between the runlevels.	Cause: The PATH variable is not set properly or permission is not granted to the user to switch between runlevels. Solution: Check whether the user is granted the necessary privileges required to change the runlevel or if the path of the/sbin directory is set in the PATH variable.

Core System Variables

Core system variables affect the behavior of applications and commands. Some of the system variables and their functions are given in the following table.

Use This Variable	If You Need To Specify
HOSTNAME={hostname}	The hostname of the system.
SHELL={shell path}	The shell path for the system.
MAIL={mail path}	The path where mail will be stored.
HOME={home directory}	The home directory of the user.
PATH={user path}	The path in which the user needs to operate.
HISTSIZE={number}	The number of entries to be stored in the history.
USER={user name}	The name of the user.

Single-User Mode

Single-user mode in Linux can be initialized by changing the runlevel to 1. It is used when the system does not allow you to log in after booting. The networking feature is disabled in single-user mode, which makes it an ideal mode to troubleshoot network problems. Single-user mode can be used for filesystem checks, because most of the partitions are not mounted in runlevel 1. This mode can even be used to recover the root password.

```
sh-3.2# passwd
Changing password for user root.
New UNIX password:
Retype new UNIX password:
type=1100 audit(1248939967.762:16): user pid=3699 uid=0 auid=4294967295 msg='PAM
: chauthtok acct="root" : exe="/usr/bin/passwd" (hostname=?, addr=?, terminal=co
nsole res=success)'
type=1100 audit(1248939967.763:17): user pid=3699 uid=0 auid=4294967295 msg='op=
change password id=0 exe="/usr/bin/passwd" (hostname=?, addr=?, terminal=console
res=success)'
passwd: all authentication tokens updated successfully.
sh-3.2# _
```

Figure 16-2: Changing the root user password in single-user mode.

Boot Disks

Definition:

A *boot disk* contains operating system files, such as `init`, `klogd`, and `syslogd`, required to start a system. It can be a hard disk, floppy disk, CD-ROM, DVD-ROM, or USB drive. The boot disk contains configuration files, startup files, and programs. The boot disk is used to boot a system following a hard disk crash. Some distributions use the first CD in the installation set as the boot disk. Other distributions allow you to create a floppy disk that can be used to boot the system.

Example:

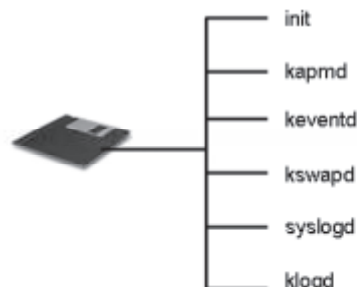


Figure 16-3: Contents of a boot disk.

Ramdisks

A ramdisk is a portion of memory that is allocated and used as a partition. The memory allocated as ramdisk is treated as a hard drive. Frequently accessed files can be placed in the ramdisk, which in turn will increase the performance of the system.

The ramdisk word Keyword

The `ramdisk` word keyword is a keyword that specifies the location of the root filesystem. The `ramdisk` word can be set and accessed using the `rdev` command.

The boot.iso File

The `boot.iso` file is an ISO-9660 image that is used to create bootable CD- or DVD-ROMs. This image file can be burned on to a CD-ROM, which can then be used for installing Linux, just like the original installation media itself. The boot speed of CD-ROMs is also an added advantage.

The diskboot.img File

The `diskboot.img` file is a VFAT filesystem image that is used to create bootable USB pen drives. Once the image is written onto the USB, it can then be used as a media for Linux installation. However, using a USB to boot a system depends on the BIOS settings. The `diskboot.img` image file should be written onto the USB using the `dd` command.

Root Disks

Definition:

A *root disk* contains directories, such as `etc`, `bin`, `home`, and so on, which contain files required to run a Linux system. It need not contain a kernel or a boot loader. The root disk can run a system without depending on any other disk.

Example:

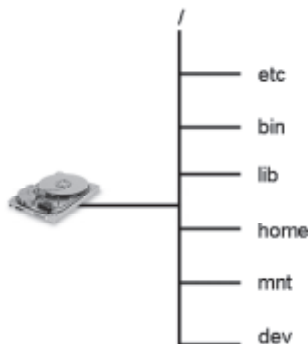


Figure 16-4: Various components of the root disk.

Zero-Filled Files

There are times when you might need to create a filesystem that does not contain any data or partition table. One of these times might be when you need to build a compressed root filesystem. To do this, you need to create a zero-filled file, partition, or ramdisk. The `dd` command can be used to create a zero-filled file or partition, which overwrites the disk with zeroes, effectively wiping out all data. This command erases data and partition tables, if any. By creating the zero-filled file or partition, you will be able to compress a filesystem to the maximum.

Kernel Panic

If a user is unable to boot a system, it may be due to disk errors caused by hardware devices. When the “Kernel Panic” message is displayed, the filesystem is corrupted or inaccessible. To resolve this issue, log in to rescue mode and perform an integrity check on the filesystem.

How to Troubleshoot Linux-Based Issues

Procedure Reference: Analyze a Problem by Gathering Data

To analyze a problem by gathering data:

1. Log in as root in the CLI.
2. Gather data about the issue using appropriate commands and files.
 - To analyze the history of commands run by the user, enter `history`.
 - To find the specified keyword in the log file while troubleshooting, enter `grep {keyword} {log file name}`.
 - To view if there are any changes in the file compared with the last backed up state, enter `diff {current file} {backed up file}`.

- To find all the files that were modified within a specified timing, enter `find {location of the directory to search} -cmin {time in minutes}`.
- To collect more information when the specified command is run, enter `strace {command}`.
- To list all open files of all active processes in a system, enter `lsof`.
- To view the log file as and when it is updated, enter `tail -f {log file name}`.
- Configure system logs to log all debug messages.
 - a. To open the system log configuration file, enter `vi /etc/syslog.conf`.
 - b. To set the type and level of severity to be logged in the specified file, type `{facility} {level of severity} {file where the log messages will get stored}`.
 - c. Save and exit.
 - d. To restart the system log service and apply the changes, enter `service syslog restart`.

Troubleshooting the Boot Process

Cause	Solution
If the boot loader screen does not appear, then GRUB may not be properly configured.	Configure the <code>/boot/grub/grub.conf</code> file in rescue mode.
If the grub> prompt appears, then GRUB may be corrupted.	Install GRUB again in rescue mode.
If the kernel does not load, then the kernel image may be corrupted.	Install a new kernel in rescue mode.
If the kernel does not load, then the parameter passed during the system start up may be wrong.	Specify the correct parameter by editing GRUB on the boot loader screen.
If there is a kernel panic, then: <ol style="list-style-type: none"> 1. The boot loader may have been misconfigured. 2. The <code>/etc/inittab</code> file is misconfigured. 3. Or, the root filesystem is misconfigured. 	<ol style="list-style-type: none"> 1. In rescue mode, configure the boot loader configuration. 2. In rescue mode, define parameters in the <code>/etc/inittab</code> file correctly. 3. In rescue mode, run a filesystem check on the filesystem.
If the kernel loads, but <code>/etc/rc.d</code> causes an issue, then the <code>/etc/fstab</code> file may have an error.	In rescue mode, fix the <code>/etc/fstab</code> file.
If the kernel loads, but <code>/etc/rc.d</code> causes an issue, then the <code>fsck</code> utility may have failed.	In rescue mode, run the <code>fsck</code> command manually.
If the services do not start correctly, then they may not have been configured properly.	Configure the services properly.

Procedure Reference: Use the Linux Rescue Environment

To use the Linux rescue environment:

1. To boot from the recovery disc, modify the BIOS settings.
2. Insert the first Red Hat installation CD into the CD-ROM drive and boot the system.
3. To enter rescue mode, at the boot prompt, enter `linux rescue`.
4. If necessary, to access the installation files, specify settings as necessary.
 - a. Specify the language and keyboard settings.
 - b. On the **Setup Networking** page, select **Yes**.
 - c. On the **Network Configuration** page, specify the networking parameters or **eth0** and then select **OK**.
5. A message is displayed, stating that the root partition will be mounted in the `/mnt/sysimage` directory. To mount the filesystem with read and write permissions, select **Continue**.
6. To continue with the boot process, select **OK**.
7. The root directory is now mounted on the ramdisk. To change the root directory to the one mounted in the `/mnt/sysimage` directory, enter `chroot /mnt/sysimage`.
8. Troubleshoot to find the cause of system failure and make the necessary changes to recover the system.
9. To exit the chroot environment, enter `exit`.
10. Enter `sync` so that the changes you made are reflected in the filesystem on the hard disk.
11. To exit from rescue mode, enter `exit`. The system will now reboot.

ACTIVITY 16-1

Troubleshooting GRUB

Before You Begin:

- 1. On srvB, you have logged in as root in the CLI.
- 2. To open the GRUB directory, at the command line, enter `cd /boot/grub`.
- 3. To back up the existing GRUB configuration file, enter `cp grub.conf grub1.conf`.
- 4. To open the current GRUB configuration file, enter `vi grub.conf`.
- 5. Comment all the lines.
- 6. Save and close the file.
- 7. To apply the settings, enter `reboot`.

Scenario:

Your system boots with the **grub** prompt rather than booting from the **GUI** prompt. Even after reboot, the situation remains the same. This indicates that there is an issue with the GRUB configuration. You prefer the system to boot through the GUI.

What You Do	How You Do It
1. Correct the GRUB settings.	<ul style="list-style-type: none">a. At the grub prompt, enter rootb. To view the current boot loader settings, enter cat /boot/grub/grub.confc. Make a note of the kernel and module settings.d. To clear the terminal screen, enter cleare. Enter kernel /boot/vmlinuz-2.6.18-128.el5 ro root=LABEL=/ rhgb quietf. Enter initrd /boot/initrd-2.6.18-128.el5.imgg. To reboot the system, at the grub prompt, enter boot

LESSON 16

2. Check the corrected grub.conf file to ensure that the settings are correct.
 - a. To switch to the CLI, press **Ctrl+Alt+F1**.
 - b. Log in as **root** in the CLI.
 - c. To navigate to the grub directory, enter **cd /boot/grub**
 - d. To delete the current GRUB configuration file, enter **rm grub.conf**
 - e. To confirm the remove action, enter **y**
 - f. To replace the correct GRUB configuration file, enter **mv grub1.conf grub.conf**
 - g. To view the current grub.conf file, enter **cat grub.conf**
 - h. To clear the terminal screen, enter **clear**
-

ACTIVITY 16-2

Troubleshooting Partitions

Before You Begin:

1. On srvB, you have logged in as root in the CLI.
2. To change to the root directory, enter **cd /root**.
3. To change the filesystem label, enter **e2label /dev/sda2 /boo**.
4. To apply the settings, enter **reboot**.



The partition may vary according to your system. For example, it may be hda2 or sda3. In such cases, suitably modify the instruction to match your system.

Scenario:

A new employee, Jim, accidentally changed some system files. When he tried booting the machine, he gets the error message “Checking filesystems. fsck.ext3: Unable to resolve ‘LABEL=/boo’.”

What You Do	How You Do It
1. Troubleshoot the partition label issue.	<ol style="list-style-type: none">At the command prompt, enter the root password.To view the label entries of all the partitions, at the Repair filesystem prompt, enter cat /etc/fstabTo view the boot device information, enter fdisk -lObserve that the boot device partition is /dev/hda2.To check if the label name is the same as that in the /etc/fstab file, enter e2label /dev/hda2Observe that the boot directory information is specified as /boo instead of /boot.To rectify the mistake in labeling, enter e2label /dev/hda2 /bootTo reboot the system, press Ctrl+D.
2. Check whether the system recovered.	<ol style="list-style-type: none">Verify that the system reboots and the GUI login screen is displayed.Log in as root in the GUI.

ACTIVITY 16-3

Troubleshooting Runlevels

Before You Begin:

- 1. On srvB, you have logged in as root in the GUI.
- 2. Switch to the CLI terminal.
- 3. Log in as root in the CLI.
- 4. To access the inittab file containing runlevel information, enter `vi /etc/inittab`.
- 5. Comment the line that starts with “si::sysinit:/etc/rc.d/rc.sysinit.”
- 6. Save and close the file.
- 7. To apply the settings, enter `reboot`.

Scenario:


You are requested to troubleshoot a system that is unable to boot and displays the error message “/etc/rc5.d/S00microcode_ctl: microcode device /dev/cpu microcode does not exist.” You identify that there is a system initialization error with the rc.d settings.

What You Do	How You Do It
1. Troubleshoot runlevels using the RHEL boot CD-ROM.	<ul style="list-style-type: none">a. Insert the RHEL 5 Rescue CD in the CD/DVD drive and reboot the system.b. To switch to Linux rescue mode, at the boot prompt, enter linux rescue
2. Select the language and keyboard configuration options.	<ul style="list-style-type: none">a. On the Choose a Language page, in the language selection list box, verify that the English option is selected, press Tab and press Enter.b. On the Keyboard Type page, in the keyboard type section, verify that the us option is selected, press Tab and press Enter.

3. Configure network settings and enter the rescue mode.
 - a. In the **Setup Networking** message box, verify that the **Yes** option is selected and press **Enter**.
 - b. In the **Configure Network Interface** message box, verify that the **Yes** option is selected and press **Enter** to configure the eth0 network interface on the system.
 - c. On the **Network Configuration for eth0** page, to select the **Enable IPv4 support** option, press the **Spacebar**, press **Tab** two times, and press **Enter**.
 - d. On the **IPv4 Configuration for eth0** page, select the **Manual address configuration** option.
 - e. In the **IP Address** text box, type the IP address of your system.
 - f. Press **Tab** and in the **Prefix (Netmask)** text box, type **255.255.255.0** and then to move to the next page, press **Tab** and press **Enter**.
 - g. To move to the next page, on the **Miscellaneous Network Settings** page, press **F12**.
 - h. On the **Error With Data** page, verify that **Continue** is selected and press **Enter** to ignore the error.
 - i. On the **Error With Data** page, verify that **Continue** is selected and press **Enter** to ignore the error.
 - j. On the **Rescue** page, verify that **Continue** is selected and press **Enter** to proceed to the next step.
 - k. On the **Rescue** message box, verify that **OK** is selected and press **Enter**.
-

LESSON 16

4. Troubleshoot inittab settings.
 - a. To mount the rescue environment files, at the **sh-3.2** prompt, enter **chroot /mnt/sysimage**
 - b. To go to the inittab file, enter **vi /etc/inittab**
 - c. To go to the sysinit line, enter **/#si**
 - d. To switch to insert mode, press **I**.
 - e. Observe that the cursor is at the beginning of the line **# si::sysinit:/etc/rc.d/rc.sysinit**.
 - f. To remove the comment declaration, delete the **#** symbol at the beginning of the line.
 - g. To exit command mode, press **Esc**.
 - h. Save and close the file.

 Eject the rescue CD manually from the CD-RW drive before rebooting the system.
 - i. To exit the chroot environment, enter **exit**
 - j. To reboot the system, enter **reboot**
 - k. Observe that the system boots correctly and the GUI login screen is displayed.
 - l. Log in as **root** in the GUI.
-

TOPIC B

Troubleshoot Hardware Issues

In the last topic, you corrected system-based issues in a Linux system. In addition to the system itself, hardware devices may get corrupted and may not work properly. In this topic, you will troubleshoot hardware issues.

Systems may be connected to external devices such as speakers or modems. Sometimes, these devices may not work properly. Finding the cause of the problem and fixing it will help you solve hardware issues and keep systems functioning smoothly.

Troubleshooting Tools

There are many troubleshooting tools that you can use, depending on the type of the problem you are facing and the environment in which you are working. Some of these tools are described in the following table.

Tool	Description
dmesg	A system administration command that is used to examine and control the kernel initialization process. It is used to print messages about the status of various hardware devices on the system during kernel initialization. Status messages can also be accessed from the <code>/var/log/dmesg</code> file.
/dev	A file that is used to create a boot or recoverable disk.
GNU Parted	A program that allows you to create, destroy, resize, move, and copy hard disk partitions.
HardDrake	A service that provides hardware detection in a graphical interface.
KNOPPIX	A bootable CD (or DVD) that contains GNU/Linux software, which includes automatic hardware detection and support. KNOPPIX can be used as a rescue system.
ifconfig	A file that is used to view the IP address and subnet mask and verify that they are allocated. It can also be used to debug or tune a system.
/proc	The proc filesystem is a pseudo-filesystem that is used as an interface to the kernel data structures. Each process contains a subdirectory in the <code>/proc</code> directory.

LNK-BBC

LNK-BBC is a Linux distribution that is small enough to fit in a CD-ROM, which is the size and shape of a business card. LNK-BBCs can be used to rescue damaged machines or as a temporary Linux workstation. More information regarding LNK-BBC can be found at <http://www.lnk-bbc.com>.

Starting and Stopping Processes to Locate and Correct Problems

Both services and processes can be stopped and restarted. This can sometimes be used to fix problems. You can use the `ps` command along with the `grep` command to locate processes that you need to check on. You can then kill the processes if necessary.

The `pgrep` command is used to look up or signal processes based on their names or other attributes. It looks through the running processes and lists PIDs that match the criteria you specify. For instance, the `pgrep -u root sshd` command lists only processes called `sshd` and that are owned by the `root` user. The command `pgrep -u root,daemon` lists all processes owned by `root` or `daemon`.

The `pkill` command can be used in conjunction with the `pgrep` command to stop processes. Starting and stopping processes is just one more way to troubleshoot problems. When you see a certain symptom, such as a process taking too long, you should first check on the process using the `ps` or `pgrep` command; then if necessary, end the process using the `kill` or `pkill` command. You should next examine the process (the script or other command sequences associated with that process) and check for any problem. After fixing the problems, you should try running the command or script again. Check on it periodically to see if it is working properly.

Hardware Problems

Hardware devices may experience failures anytime while the system is being used.

Symptom	Cause and Solution
The user is unable to hear from the speakers.	Cause: The speaker or the sound card is not functioning properly. Solution: Check the speaker and its corresponding driver. If you still have a problem, then you need to check the sound card.
The modem is unable to dial in or out.	Cause: There is a mismatch between the modem configuration and the modem settings, or there could be a modem failure. Solution: Check the modem and serial port settings. If the problem continues, check the corresponding drivers.
When the system boots, the monitor switches to power save mode or the power light flickers.	Cause: The CPU is unable to establish a link with the monitor. Solution: Check if the monitor cable is connected to the system and then check the functionality of the VGA card.
The dumb terminal device is unable to boot. It just stops with the display screen.	Cause: The dumb terminal is unable to connect with the server. Solution: Check the serial ports and cables.
A system connected to the UPS shuts down abruptly.	Cause: The UPS is malfunctioning, or there is a mismatch between the UPS settings and the configuration file. Solution: Check the serial ports, the cable, and the configuration file.
The user is unable to switch to GUI mode.	Cause: The mouse does not function properly due to the configuration settings or there could be a problem in the device. Solution: Unplug and reconnect the mouse, then restart the system.

Symptom	Cause and Solution
The user is unable to access the floppy or the CD drive.	<p>Cause: The driver is not mounted or there is some problem with the driver.</p> <p>Solution: Check whether the read/write indicator is on. Otherwise, check the power cable connected to the drive.</p>

Viewing Hardware Details

Some commands that are frequently used for viewing hardware details are listed in the table.

Command	Used To
<code>dmesg</code>	View bootup messages.
<code>/sbin/lspci</code>	View information about PCI cards.
<code>lsdev</code>	View information about the installed hardware.
<code>/sbin/lsmmod</code>	View a list of loaded modules.
<code>/bin/uname</code>	View system information such as the kernel name, release and version numbers, hardware platform, and operating system.

How to Troubleshoot Hardware Issues

Procedure Reference: Troubleshoot Sound Card Issues

To troubleshoot sound card issues:

1. Verify that the speaker is connected, switched on, and is functioning.
2. If the speaker is functioning but the problem persists, verify that the sound card is detected while booting.
 - a. Verify that the sound card is listed in the output of the `lspci` command.
 - b. If the sound card is not detected, contact your hardware engineer to resolve the sound card issue.
3. If the sound card is detected and the problem still persists, verify that the sound card module is loaded.
 - a. Verify that the sound card module details are listed in the output of the `lsmod` command and `lsmod {module name}` command.
 - b. If the sound card module is not loaded, add an entry for the sound card in the `/etc/modprobe.conf` file. To add an entry in the file, you need to know the slot number and the name of the module used for the sound card and specify it in the format, `alias sound-slot-{slot number} {module name}`.



The `/lib/modules/[kernel version]/kernel/sound` directory contains modules for the sound card.

- c. To load the module automatically, reboot the system.



You can also load the module using the `modprobe` or `insmod` command. If you want to use the `modprobe` command, run the `depmod` command to build or update a module database.

Procedure Reference: Troubleshoot Modem Issues

To troubleshoot modem issues:

1. Verify that the modem is connected properly to the system and powered on.
2. Check your telephone line and verify that it is connected properly to the modem.
3. Verify that the modem speed is set properly.
 - a. Verify that the modem speed specified in the `/etc/mgetty+sendfax/mgetty.config` file is equal or less than your modem speed.
 - b. If the modem speed is not set, modify the `speed` parameter in the file, and set the speed in the format, `speed {speed in bps}`.
4. Verify that the serial port settings are correct.
 - a. Verify that the settings listed in the output of the `setserial -a /dev/ttyS0` command matches with your modem specifications.
 - b. If the serial port settings are not proper, change them, using the commands, `setserial /dev/ttyS{port number} {spd_normal | spd_hi | spd_vhi}` and `setserial /dev/ttyS{port number} baud_base {baud rate}`.
5. If you are still unable to dial using the modem, then the issue is hardware related. Contact your hardware engineer to resolve the issue.

Procedure Reference: Troubleshoot LCD Panel Issues

To troubleshoot LCD panel issues:

1. Verify that the LCD panel is connected to the system properly and is powered on.
2. Verify that the VGA card module is configured correctly.
 - a. Verify that all the parameters in the **Screen** section in the `/etc/X11/xorg.conf` file are entered correctly.
 - b. If necessary, modify the parameters according to your LCD panel specifications.
3. Verify that the monitor parameters such as `DefaultDepth`, `Viewport`, and `Depth` are configured correctly.
 - a. In the `/etc/X11/xorg.conf` file, verify that the `DefaultDepth`, `Viewport`, and `Depth` parameters are set properly.
 - b. If necessary, modify the parameters according to your LCD panel specifications.
4. If the LCD monitor is still not working properly, then the issue is hardware related. Contact your hardware engineer to resolve the issue.

Procedure Reference: Troubleshoot Dumb Terminal Issues

To troubleshoot dumb terminal issues:

1. Verify that the dumb terminal device is connected properly to the server.
2. Verify that the serial port is configured correctly.
 - a. Verify that the settings listed in the output of the `setserial -a /dev/ttyS0` command matches your device specifications.
 - b. If necessary, change the serial port settings, using the commands,


```
setserial /dev/ttyS{port number} {spd_normal | spd_hi |
spd_vhi} and
setserial /dev/ttyS{port number} baud_base {baud rate}.
```
3. If the dumb terminal is still not working properly, then the issue is hardware related. Contact your hardware engineer to resolve the issue.

Procedure Reference: Troubleshoot Issues Related to UPS Devices

To troubleshoot issues related to UPS devices:

1. Verify that the UPS device is connected properly to the server.
2. Verify that the serial port is configured correctly.
 - a. Verify that the settings listed in the output of the `setserial -a /dev/ttyS0` command matches your device specifications.
 - b. If necessary, change the serial port settings, using the commands,


```
setserial /dev/ttyS{port number} {spd_normal | spd_hi |
spd_vhi} and
setserial /dev/ttyS{port number} baud_base {baud rate}.
```
3. If the UPS device is still not working properly, then the issue is hardware related. Contact your hardware engineer to resolve the issue.

Procedure Reference: Troubleshoot Mouse Issues

To troubleshoot mouse issues:

1. Verify that the mouse is connected properly to the system.
2. Reboot the system.
3. If the mouse is still not working, then the issue is hardware related. Contact your hardware engineer to resolve the issue.

Procedure Reference: Troubleshoot Floppy Disk Problems

To troubleshoot floppy disk issues:

1. Verify that the power connector to the floppy drive is connected and working.

If the connection is not powered on, then there is a problem with the power connector.

- a. Verify that the read-write indicator is glowing.
- b. If it is not glowing, the power connector needs to be checked and replaced.

2. If the power connector is working and the floppy issue persists, then there is a problem with the floppy drive or the floppy.
 - a. With your hardware engineer's help, verify that the floppy drive is functioning properly.
 - b. If the floppy drive is functional, verify that your floppy is functioning properly.

Procedure Reference: Troubleshoot X

To troubleshoot X:

1. Switch to runlevel 3.
2. Check whether the required criteria for X are met.
 - Ensure that the quota value for the user has not been reached.
 - To check whether the xfs font server is running, enter `service xfs status`.
 - To gather more information, enter `X -probeonly`.
 - Make sure that the hostname of the system is configured properly.
 - To check whether the display settings are configured properly, enter `system-config-display`.

Procedure Reference: Troubleshoot Printing Problems

To troubleshoot printing problems:

1. Verify that the printer cables are connected properly and the power source is switched on.
2. Verify that the paper trays are stocked.
3. To verify that the printer daemon is running, enter `service cups status` and, if the daemon service is not running, enter `service cups start`.
4. Check the status of the print job in the queue.
 - a. In the CLI or in the GUI terminal window, enter `lpq -P {print queue name}`.
5. To restart the CUPS service, enter `service cups restart`.
6. To verify that the print job is getting executed, enter `lpr {file name}`.

DISCOVERY ACTIVITY 16-4

Troubleshooting Hardware Issues

Scenario:

Your company organized a trade show, where you set up several dumb terminals with LCD monitors to demonstrate your company's products. You are responsible for troubleshooting any hardware-related issue.

1. In which file will you change the LCD monitor parameters such as DefaultDepth, Viewport, and Depth?
 - a) /etc/x11Config
 - b) /etc/XF86
 - c) /X11/XF86Config
 - d) /etc/X11/xorg.conf

 2. One of the LCD monitors is not displaying any output. What could be the problem? Select all that apply.
 - a) The LCD panel is not connected properly to the system.
 - b) The VGA card module is not configured properly.
 - c) Serial port settings are not configured properly.
 - d) Monitor parameters, such as DefaultDepth, Viewport, and Depth, are not configured properly.

 3. True or False? In the /etc/X11/xorg.conf file, the Screen section contains parameters of the VGA card module for an LCD monitor.
☐ True
☐ False

 4. In one of the terminals, users are not able to listen to the audio associated with the animation. What will be your first step to troubleshoot the issue?
 - a) Verify that the sound card is detected while booting.
 - b) Verify that the sound card module is loaded.
 - c) Contact the hardware engineer to solve the issue.
 - d) Verify that the speaker is connected, switched on, and working properly.

 5. Which command will you use to verify serial port settings?
 - a) setserial -q
 - b) setserial -v
 - c) setserial -a
 - d) setserial -z
-
-

TOPIC C

Troubleshoot Network Connection and Security Issues

In the previous topic, you identified and solved system- and hardware-based issues in Linux. In a networking environment, Linux systems will be prone to connection- and security-related issues. You need to continually identify and prepare for vulnerabilities. In this topic, you will troubleshoot network connection and security issues.

Security encompasses a number of different aspects; from passwords and permissions to data encryption, firewalls, and even physical security. Despite all this protection, if you are not aware of the symptoms that lead to security breaches, or if you are not familiar with steps required for repairing corrupted files, your network will remain open and vulnerable to potential attacks.

Network Issues

If users are unable to connect to a network, they will not be able to log in to their systems or access the services or shared resources. Network problems can be categorized as hardware-related issues and service-related issues. Hardware-related network issues can be solved by checking the network devices, including the network cable and the network card. Service-related network issues can be fixed by checking the network settings of a system or the server.

Network Troubleshooting Utilities

The `tracert`, `ping`, and `arp` utilities are very useful in troubleshooting issues related to remote network services.

Utility	Used To
<code>tracert</code>	<p>Track the route data that it takes to get to its destination. Utilizing the TTL field of the IP protocol, <code>tracert</code> attempts to obtain an ICMP Time_Exceeded response from each gateway encountered on the path between the sender and the final destination.</p> <p>UDP probe packets are sent with a short TTL. The <code>tracert</code> utility then listens for an ICMP Time_Exceeded reply from a gateway. This continues until you can get an ICMP Port_Unreachable response, which means that you either got to the host or reached the default maximum number of hops (30). The address of each system that responds (each gateway you pass through) is printed to your screen; if no response is received within five seconds, an asterisk (*) is printed for that probe.</p>

Utility	Used To
ping	Verify that a system can be reached on a network. It checks the hostname, the IP address, and whether the remote system can be reached. Ping uses the ICMP Echo_Request datagram to check connections among hosts, by sending echo packets and then listening for reply packets.
arp	Display information, such as the hardware address, the hostname, and the network interfaces, about the <i>Address Resolution Protocol (ARP)</i> cache.

ARP

Address Resolution Protocol (ARP) is a network protocol that is used by IP to map network addresses to MAC addresses.

Symptoms of Network Security Problems

There are a variety of ways that security can be compromised on a system. It is recommended that you check the Linux log files before troubleshooting. Some symptoms that indicate potential security problems include:

- Disruption or Denial-of-Service (DoS).
- Unauthorized system use for processing data.
- Unexplained system hardware changes.
- Theft (data information and vandalism).
- Unusual software characteristics.
- And, suspected virus outbreak.

Security Tips

Avoid using authentication methods based solely on IP addresses. Keep network packages up to date, and be aware of the new versions of programs such as BIND, Postfix, and SSH. Disable unnecessary network services.

System Security Monitoring Tools

Various tools can be used to effectively monitor a system for any security issue and identify symptoms.

Tool	Description
System Log Files	There are three types of system log files that can help in monitoring system security: Log: This file contains information about connections established and files transferred. Stats: This file lists file transfer statistics. Debug: This file contains debugging information and login and password information for remote system connections.

Tool	Description
Central Network Log Server	The reports generated from the server contain useful information on server logs and online alerts, which can be analyzed for identifying security breaches or threats.
chkconfig	This utility can be used to check configuration files and update and query runlevel information for system services.

Network Security Vulnerabilities

Although Linux is considered a secure operating system, a network of systems can still have unauthorized users gaining access. Once an attacker gains access to a system, almost any security system can be compromised.

Vulnerabilities include:

- Proliferation of worms and viruses via email messages.
- Malicious execution of programs by a user with root privileges.
- Potential hole in the Linux kernel.
- Passwords that can be easily deciphered.
- Services running on the system such as FTP, SMB, Sendmail, and SNMP.
- Domain spoofing.
- DNS servers running vulnerable versions of BIND.
- And, Remote Procedure Calls (RPCs).

IP Spoofing

IP spoofing is a technique for changing, or spoofing, your IP address in order to fool the target system into believing that your IP identity is actually another system with the spoofed address.

Software Vulnerabilities

Software vulnerabilities account for many successful attacks because attackers are opportunistic. They exploit well-known flaws using the most effective and widely available attack tools. They also count on organizations that do not fix the problems and scan the Internet for vulnerable systems.

BIND Attack

In a BIND attack, an intruder can erase your system logs and install tools to gain administrative access. In addition, once the attacker has gained access, he or she uses the attacked system to scan for and attack other network systems running vulnerable versions of BIND. In effect, the intruder uses the compromised system to attack hundreds of remote systems, resulting in additional successful compromises.

Sendmail Flaws

Over the years, flaws have been found in Sendmail. In one of the most common intrusions, the attacker sends a crafted mail message to a machine running Sendmail. Sendmail, in turn, interprets the message as instructions requiring it to send the password file to the attacker's machine.

SNMP Flaws

SNMP uses an unencrypted community string as an authentication mechanism, and the default community string used by many SNMP devices is public. Sniffed SNMP traffic can reveal information about the structure of your network, as well as the systems and devices attached to it.

Honeypot Systems

A system designed to attract attackers is known as a *honeypot*. If an attacker manages to get past your packet filter and starts scanning for options, the honeypot should be the system configured to look like it is vulnerable to known attacks. A honeypot system should not be too easy to spot because a savvy intruder will be tempted to look further on the network.

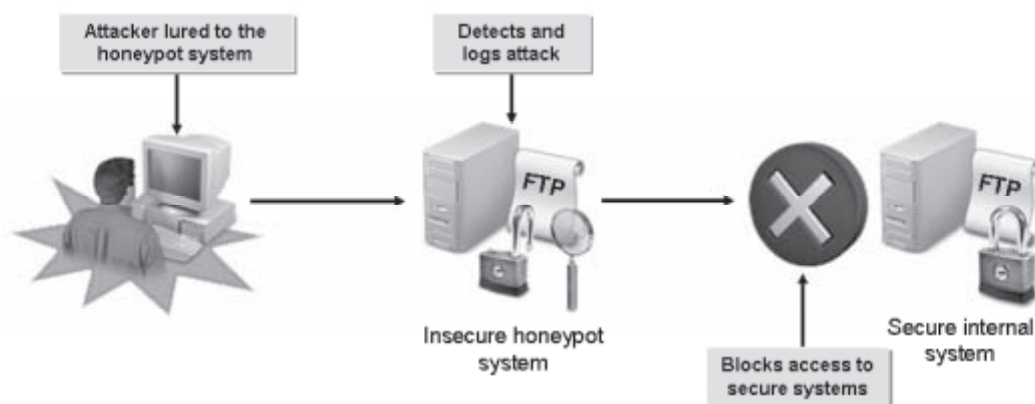


Figure 16-5: The functioning of a honeypot.

Goals of a Honeypot

There are several goals for a honeypot:

- To provide a lure so that attackers stay away from other equipment. You want the attackers to see a vulnerable system that they know they can exploit and gain access to. This system needs to be such that the attacker focuses his or her energy on exploiting the system, as opposed to the server with important data that is sitting right next to it.
- To know that the honeypot system will be attacked, so that you can take extra measures when logging in to it. These logs should be moved off the system frequently—perhaps hourly or daily if your network is a high-profile target.
- To increase the ability to detect and respond to incidents. The theory is that if you are aware of what the attacker is doing to your honeypot, you can be better prepared to defend or, if possible, prevent the attack on your production systems.

Legal Issues Regarding Honeypots

Be aware that there may be legal issues surrounding the use of the honeypot technology. The intentional setup of a honeypot may be considered entrapment, and therefore the same rules apply as in the real world.

Another issue is that of privacy. If an attacker were to set up an IRC server on the honeypot, it will be possible to log all conversations on that server. There is currently no defined law explicitly regarding this subject. However, it should be noted that an attorney could make privacy a viable defense argument.

Guidelines for Troubleshooting Network Issues

When troubleshooting a network problem, well-established guidelines help you narrow down the cause of the problem and map steps toward its resolution.

Guidelines:

To troubleshoot a network problem:

1. Define the problem and gather the facts.
2. If possible, re-create the problem.
3. Consider all possibilities.
4. Create and implement an action plan.
5. Observe and document results.
6. Provide feedback.

Example: Troubleshoot a Network Problem

You have a client system that is unable to access a server. As the first step, you ping the server and realize that you do not receive a response. After that, you use `tracert` to determine how far down the line the problem is occurring. You discover that the problem is in the router. You take corrective action, document the results, and inform the user that the server is once again accessible.

How to Troubleshoot Network Connection and Security Issues

Procedure Reference: Troubleshoot Network Issues

To troubleshoot network issues:

1. Verify that the network cable is plugged in properly.
2. To find out more information about the error, view the `/var/log/messages` file.
3. Verify that the network service is available for the runlevel you are in.
 - a. Verify that the network file is present in the `/etc/rc.d/rc{runlevel}.d` directory.
 - b. If the file is not present, to enable the network service in the runlevel, enter the `chkconfig --level {runlevel} network on` command.
4. Verify that the network service is started.
 - a. To view the status of the network service, enter `service network status`.
 - b. If the service is stopped, to start it, enter `service network start`.
5. Verify that the IP address and subnet mask are allocated by viewing the output of the `ifconfig` command.
 - a. To view the IP address and subnet mask, enter `ifconfig`.
 - b. If no entries for the IP address and subnet mask are displayed, determine if the IP addresses are allocated manually or through a DHCP server.
 1. If IP addresses are allocated through a DHCP server, change the **BOOTPROTO** parameter to **dhcp** in the `/etc/sysconfig/network-scripts` file.

2. If IP addresses are allocated manually, verify that the **IPADDR** and **NETMASK** parameters are set in the `/etc/sysconfig/network-scripts` file.
3. Restart the network service.
- c. To verify that you are able to connect to the network, ping the network gateway using the command, `/bin/ping {IP address}`.
6. Verify that the default gateway and routing table are configured properly.
7. Verify that the name-to-IP address resolution on your network is working properly.
 - If you implemented DNS on your network, verify that the DNS entries are correct.
 - a. Using the `host`, `dig`, or `nslookup` commands, verify that the name-to-IP address mapping is correct in the DNS configuration files.
 - b. `dig {host name or FQDN}`.
 - c. `host {host name or FQDN}`.
 - d. `nslookup {host name or FQDN}`.
 - If you have not implemented DNS on your network, verify that the `/etc/hosts` file has correct name-to-IP address mapping information.
8. Verify that IP forwarding is enabled.
 - a. Verify that the `/proc/sys/net/ipv4/ip_forward` file has the value 1.
 - b. If the file contains 0, change the value to 1.
 1. In the `/etc/sysctl.conf` file, modify the value of the **net.ipv4.ip_forward** parameter to 1.
 2. Run the `sysctl` command to apply the changes in the `sysctl -p /etc/sysctl.conf` file.
9. Verify that the ports of the service you are trying to access are open at the destination host.
 - a. Use Telnet to access the service through a specific port, `telnet {host name} {port number}`.
 - b. In the `/etc/hosts.allow` and `/etc/hosts.deny` files and iptables, verify that you are allowed to access the ports.
 - c. If the port is not open, start the service by using the `service {service name} start` command or by adding an entry for the startup script in the `rc.local` file.
10. Verify that the hostname is set.
 - a. Display the hostname by using the `hostname` command.
 - b. If the hostname is not set, to add an entry for the host, modify the `/etc/sysconfig/network` file.

Procedure Reference: Troubleshoot Security Issues

To troubleshoot security issues:

1. Check your newly created `/var/log/iptables` log file for intrusion attempts.
2. Check the `/var/log/messages` file for errors.
3. Check the `/var/log/secure` file for errors.

DISCOVERY ACTIVITY 16-5

Troubleshooting Network Issues

Scenario:

You recently received a lot of trouble tickets, all of which are related to network connections. You need to check the cause of these network issues and troubleshoot them.

1. One of your network users is unable to connect to the FTP server, which is located on a different network. The error message indicates that the other network is unreachable. You verified that the network cable is intact and that the FTP server is up. What could be the probable cause of the error? Select all that apply.
 - a) The network service is not up.
 - b) The resolv.conf file does not contain entries for the name server.
 - c) Network parameters, such as the IP address, the subnet mask, or the default gateway, are not set correctly.
 - d) The firewall is disabled.
 2. You verified that the network service is running and that the network parameters are properly set. However, the user is still unable to connect to the network. What will be your first step to troubleshoot the network issue?
 - a) Verify that the hostname is set.
 - b) Verify that the DNS entries are correct.
 - c) Verify that IP forwarding is enabled.
 - d) Verify that the ports of the service you are trying to access are open at the destination host.
 3. True or False? To set the hostname permanently, you need to modify the /etc/sysconfig/network file.
☐ True
☐ False
-
-

Lesson 16 Follow-up

In this lesson, you acquainted yourself with the various troubleshooting strategies in Linux. This will enable you to effectively tackle most of the issues that may arise while working with Linux-based systems.

1. When will you troubleshoot the boot loader? Why?

2. Under what circumstances will you troubleshoot the system environment?

LESSON 17

Installing Linux

Lesson Time*1 hour(s), 20 minutes*

In this lesson, you will install the Linux operating system.

You will:

- Prepare for a Linux installation.
- Identify the phases of the Linux boot sequence.
- Configure the GRUB boot loader.
- Install the Linux operating system.
- Perform post-installation tasks.

Introduction

You have knowledge about all elements and services in the Linux operating system. Getting acquainted with the services and working of the Linux operating system will enable you to recognize your requirements while installing Linux. In this lesson, you will install the Linux operating system.

As a Linux professional, you have to ensure that your computer's settings and hardware configuration are sufficient for hosting Linux. Also, you need to determine the features that have to be installed to suit your requirements.

This lesson covers all or part of the following CompTIA Linux+ Powered by LPI certification objectives:

- Topic A:
 - Objective 101.1, Objective 101.2
- Topic B:
 - Objective 101.2, Objective 102.2, Objective 105.1
- Topic C:
 - Objective 101.1, Objective 102.1, Objective 102.2
- Topic E:
 - Objective 106.1

TOPIC A

Prepare for Installation

In the last lesson, you did some troubleshooting of devices to ensure the smooth operation of the entire Linux system. One easy way to optimize the performance of the Linux system is to only select peripheral and hardware devices that are fully supported by Linux. In this topic, you will perform the preparation tasks necessary for a successful installation of Linux.

Preparing for a new Linux installation is much like setting out to cook a fine meal. You need to gather all the necessary ingredients to accomplish the task. Thorough preparation will help prevent failure when attempting to boot your system for the first time.

Hardware Compatibility

The first thing you should do before purchasing any hardware component is to check whether it is on the Hardware Compatibility List (HCL) for Linux. Before you install Linux, you should gather information about your system. Much of this information is available in your system documentation. Some of the questions that you should address before purchasing a hardware component are listed in the table below.

Component	Questions To Address
Hard drive	<ul style="list-style-type: none"> • How many devices are installed? • Is it IDE or SCSI? • How large is the drive? • How many cylinders are contained on the drive?
Hard disk controller	<ul style="list-style-type: none"> • Is it IDE or SCSI? • Who is the manufacturer?
Memory	How much RAM is installed?
CD-ROM	Is the interface type IDE, SCSI, or other? (If it is not IDE or SCSI, you will need to record the make and model.)
SCSI adapter	<ul style="list-style-type: none"> • Who is the manufacturer? • What is the model?
Network card	<ul style="list-style-type: none"> • Who is the manufacturer? • What is the model?
Mouse	What type is it? (If serial, record the port to which it is connected.)
Monitor	<ul style="list-style-type: none"> • Who is the manufacturer? • What is the model? • What are the horizontal and vertical refresh rate ranges of the monitor?
Display adapter	<ul style="list-style-type: none"> • What chipset is used in the display adapter? • How much video RAM does the display adapter use?

Linux Distributor Testing

Distributors, such as Red Hat, Inc., test whether Linux operates correctly with specific hardware. After testing, they produce HCLs for each supported version. The lists include information about the hardware, but because the computer system configurations vary between what you may have and what they tested, the variations in manufacturing specifications aren't guaranteed to be compatible with any hardware. An HCL is a list of hardware that has been tested under specific conditions (usually under many conditions) and should be used as a guide, not as an absolute testament that the hardware will work perfectly straight out of the box (because your system is probably configured in a slightly different way than the test systems).

Hardware Compatibility Websites

The following Linux hardware compatibility sites will assist you in determining if your hardware will work with Linux:

- Red Hat hardware compatibility list—<https://hardware.redhat.com/>
- Mandriva hardware compatibility list—<http://hcl.mandriva.com/>
- SUSE hardware compatibility list—<http://en.opensuse.org/Hardware>
- Fedora hardware compatibility list—<http://fedoraproject.org/wiki/HCL>
- Ubuntu hardware compatibility list—<http://www.linuxhcl.org>
- Linux Mint hardware compatibility list—<http://community.linuxmint.com/hardware>

CPU Compatibility

It is also important to determine if your CPU is compatible with Linux. Certain distributions of Linux are tailored to different CPU types.

Installation on New Systems

On newer systems, the Linux installation program often automatically identifies your hardware. It is still a good idea to gather information ahead of time, just in case the program does not figure out what you have.

Gather Installation Information

Depending on your installed equipment, you may have to look for information in a variety of resources.

- One way to gather information is to view CMOS or diagnostic information available at system boot time. Cold-boot your system and display setup or diagnostic information. This is displayed in different ways on different systems. For example, on most Compaq systems, when the block cursor moves to the upper-right corner of the screen, press **F10**. On some systems, when the View Setup message (or a similar message) is displayed, you press **Delete** (or the key indicated in the message).
- Access to manuals that came with the equipment can often be one of the best ways to find out about components. Manufacturers' websites also often contain valuable information about equipment.
- If you don't have the documentation and you don't have an application or a utility to provide this information, you will need to open the hood and look inside. Many cards, boards, and components have manufacturer and model information printed on them. However, they probably will not have a guide to interpreting the jumpers' settings.
- If your workstation is to be connected to a network, you will also need information about the network address to be assigned to your computer. Some systems will have a permanent network address and others will obtain a network address each time they access the network. Contact the system or network administrator to find out how to set up your system.

Linux Installation Methods

Linux can be installed on servers and workstations using different methods.

Installation Method	Description
Local CD/DVD-ROM Installation	Linux can be installed from a set of installation CD/DVD-ROMs. It requires the system's BIOS settings to support booting from CD/DVD-ROMs. This is like a local installation and is the easiest way to install Linux.
Local Hard Drive Installation	Linux installation can be done by staging the installation files on the local hard drive.

Installation Method	Description
USB Drive Installation	Linux can also be installed through USB drives if CD/DVD-ROMs or other modes of installation are not supported by the system. To enable booting from USB drives, the <code>diskboot.img</code> file has to be copied from the <code>images</code> folder of the installation CD/DVD-ROM to the USB drive. This mode of installation also requires BIOS to support booting from USB drives.
Network-Based Installation	Linux installation can be done on networked computers by staging all the installation files on a separate server and installing it on clients' systems. The network installation server shares the installation directory with the clients via NFS, FTP, or HTTP. This method is often faster than CD/DVD-ROM-based installations. The network installation server is necessary for all network-based Linux installations.

Pre-Install Checklist

To ensure that your system is ready for Linux to be installed:

1. Collect basic system information about your computer.
2. Check the available hardware with HCL.
3. Verify that the minimum system requirements are met for the distribution you wish to install.
4. Plan the hard disk partitioning layout and the corresponding filesystems, including the size of the swap drive, depending on the physical RAM.
5. If necessary, check the installation media using the **Test the Media** option available on the Linux Installation CD.

The Anaconda Installer

The *Anaconda installer* is a program for installing Linux through the text or graphical mode. It provides step-by-step instructions to guide you through the installation process. It also enables you to partition and organize hard disks and manage RAID and LVMs. The installer provides various options to choose from and allows you to add different packages based on your operating requirements.

Initiates
installation of
Red Hat
Enterprise Linux

```
md: bitmap version 4.39
TCP bic registered
Initializing IPsec netlink socket
NET: Registered protocol family 1
NET: Registered protocol family 17
Using IPI No-Shortcut mode
ACPI: (supports S0 S1 S4 S5)
Time: tsc clocksource has been installed.
Freeing unused kernel memory: 228k freed
Write protecting the kernel read-only data: 397k

Greetings.
anaconda installer init version 11.1.2.168 starting
input: AT Translated Set 2 keyboard as /class/input/input8
input: ImPS/2 Generic Wheel Mouse as /class/input/input1
mounting /proc filesystem... done
creating /dev filesystem... done
mounting /dev/pts (unix98 pty) filesystem... done
mounting /sys filesystem... done
trying to remount root filesystem read write... done
mounting /tmp as ramfs... done
running install...
running /sbin/loader
-
```

Figure 17-1: The Anaconda installer in Red Hat Enterprise Linux 5.

LVM

Logical Volume Manager (LVM) is a software tool that is used to manage the disk storage on a computer system.

LVM-based installations give the system administrator greater control over disk management. By creating logical volumes, an administrator can group disks or partitions together into manageable chunks that are more enterprise-capable than simple partitions. Two of the major features of LVM are the ability to create logical volume snapshots and the resizing of logical volumes by absorbing or ejecting physical volumes.

- **pvcreate:** The Physical Volume Create utility prepares physical volumes to be used in logical volumes.
- **vgcreate:** The Volume Group Create tool creates and names volume groups.
- **lvcreate:** The Logical Volume Create tool creates and names logical volumes.

RAID

Redundant Array of Independent Disks (RAID) is a method that is used to store the same data in different locations on multiple hard disks of a server or a standalone disk storage system.

Partitioning Utilities

Definition:

The Linux operating system is usually installed on a partition of the hard disk. A *partition utility* is a program that is used to manage partitions on the hard disk. It enables you to create a new partition, modify the attributes of an existing partition, assign a filesystem to a partition, and delete a partition. A partition utility also enables you to specify the size of a partition and indicate whether the partition is a primary or logical partition. The most frequently used partition utility is **fdisk**.

Example: Disk Druid

Disk druid is a program used for partitioning disk drives during the installation process.

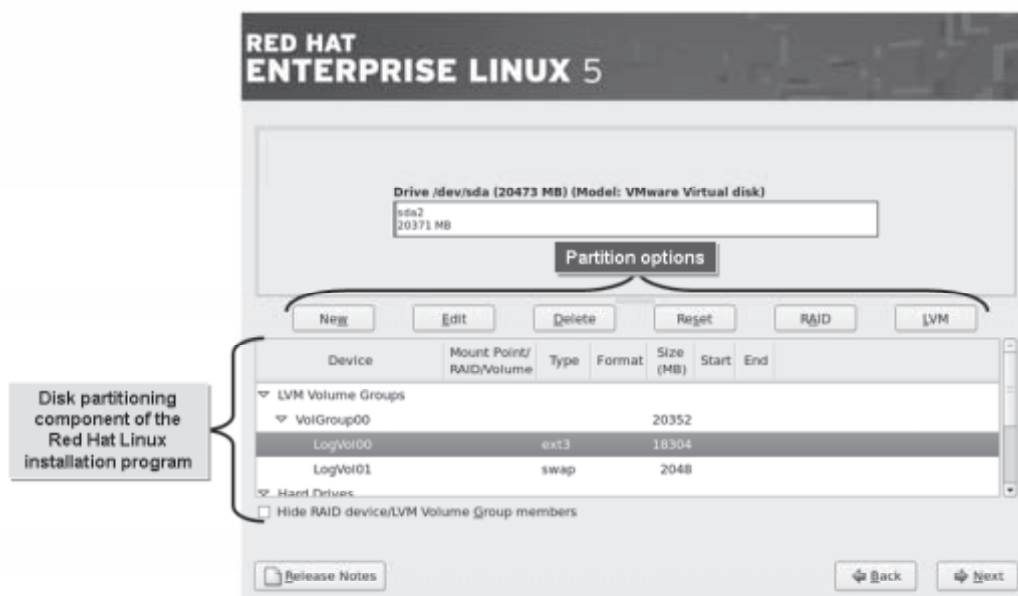


Figure 17-2: The disk partitioning component that appears during Red Hat Linux installation.

Partition Device Name

The partition device name is often `/dev/hda1` or `/dev/hda2` for IDE disks and `/dev/sda1` or `/dev/sda2` for SCSI disks.

Repartitioning Strategies

If you have neither enough free space nor a partition to spare, then you can either add another drive to install Linux or repartition your existing drive. Most DOS-based systems have a single partition that includes the entire drive. This leaves you with no space to install Linux. You can either delete the existing partition and make it smaller to accommodate Linux, or use a partitioning utility to resize it.

Unless you use a special utility, you will have to delete and then re-create partitions of appropriate sizes. In recent years, several utilities have been developed that can move partition boundaries without destroying your data.

Destructive Repartitioning

Destructive repartitioning is a traditional method. You use the `fdisk` utility to delete the existing partition, and then re-create partitions. This means that you lose all the data saved on the partition when it is deleted. Therefore, before deleting the partition, if you want to retain any information, you will need to back it up, delete and re-create the partitions, and then restore the information.

Nondestructive Repartitioning

Several third-party utilities allow you to move partition boundaries without destroying the data currently stored in the partition. This is referred to as nondestructive repartitioning. You still have to be extremely careful and follow the utilities' documentation directions exactly to avoid inadvertently destroying your data. Partition Magic and Partition-It are third-party utilities that can be purchased for this purpose.

Partitionless Installation

The partitionless installation option is available for users who want to try out Linux without installing it completely. All it requires is a formatted DOS FAT partition with enough free space for a workstation installation. However, it doesn't have all the options available that a full workstation installation would have, and you need to use a boot disk every time you want to run Linux. It is popularly known as Live CD.

The FIPS Program

The *First nondestructive Interactive Partition Splitting (FIPS)* program is a free utility that comes with some Linux distributions. It can be used to resize File Allocation Table (FAT) partitions. When running FIPS, two partitions are created: the one you resized and the one FIPS creates.

 FIPS is included on the Red Hat Linux CD-ROM in the dosutils directory.

FIPS Limitations

FIPS only works on DOS partitions with disk sector sizes of 512 bytes. Twelve-bit FATs will not be split by FIPS. Therefore, a partition will not be reduced below 4,085 clusters because this will require writing the 16-bit FAT as a 12-bit FAT. It also does not currently work with extended DOS partitions. If you already have four partitions, you cannot use FIPS to further split the partitions; FIPS requires a free partition entry with which it can work. Because of the wide variety of hardware and software configurations under which it must run, FIPS may not work properly on all systems.

BIOS

The *Basic Input/Output System (BIOS)* is a low-level firmware that acts as the interface between the hardware and the operating system on a computer. The BIOS settings can be modified according to the needs of a user. BIOS plays an important role in starting the boot process and determining the boot device settings. When a computer is powered on, BIOS is loaded into the memory, initiating the *Power-On Self Test (POST)*.

 The BIOS size varies among vendors and has a maximum size of 8 MB.

ROM BIOS

There are several BIOSes in your computer. When people say BIOS, they are generally referring to the main system BIOS. However, there are also BIOSes to control peripherals. Typically, the video card has its own BIOS, which contains hardware-driving instructions for displaying video information. SCSI host adapters, hard drives, and other peripherals can also contain their own BIOS instructions.

Plug and Play

When the main BIOS looks for the video card and other peripheral BIOSes, it will look for and configure plug-and-play devices if your BIOS supports the plug-and-play standard. When a plug-and-play device is found, BIOS displays a message on the screen prompting user input and action.

POST

POST takes an inventory of your system's hardware components in a specific order. The following table lists the components in the order in which they are tested.

Component	Description Of Test
Processor	If this test fails, the system halts without displaying any message.
ROM BIOS	A series of checksums are computed; if they don't match, the system halts.
DMA controller	If this test fails, the system halts.
Interrupt controller	If this test fails, you will hear a long beep followed by a short beep; the system then halts.
Timing chip	If this test fails, the system halts.
Video card	If this test fails, you will hear a long beep followed by two short beeps; if the test succeeds, ROM BIOS gets copied into RAM memory.
Expansion boards	Boards are initialized and, if necessary, the expansion board's ROM gets copied into the upper memory.
RAM memory	Counts and tests RAM by writing a bit to each memory bit.
Keyboard	Presence of keyboard and any stuck keys.
Floppy disk drive	Signal is sent to the adapter to activate the floppy disk drive's motor.
Other resources	Parallel and serial ports are queried; the system looks for an operating system to load.

CMOS

The *Complementary Metal Oxide Semiconductor (CMOS)* is a memory area with battery backup that is used to store system configuration settings. Prior to the use of CMOS, settings were configured with jumpers and switches. CMOS was introduced with the AT system boards. It allows more configuration options when compared to switches and jumpers. Some of the things you can configure through CMOS are:

- Password: You can specify whether a password is required following POST.
- Drive order: The order in which POST checks drives for the operating system.
- Memory: Some systems require you to specify in CMOS how much RAM is installed on the system.
- Drive type: Specifies the type of hard drive attached to the system.
- Display: Specifies the monitor type.

How to Prepare for Installation

Procedure Reference: Prepare for Installation

To prepare for installation:

1. Gather information related to your system.
 - Hardware
 - Software

- Network environment
- 2. Verify that your hardware is compatible with Linux.
- 3. Verify that the software you want to use after installing Linux will work.
- 4. Determine the purpose of the system.
- 5. Verify that your system hardware can handle the space and workload required for the purposes you need it for.

Procedure Reference: Configure BIOS to Perform Preinstallation Check on an x86 Hardware

As part of the preinstallation tasks, you need to configure the BIOS settings to ensure that the system is suitable for hosting Linux OS. To configure the system to host Linux:

1. Configure the error handling setting.
 - a. Access BIOS according to the manufacturer's instruction.
 - b. Select the **Halt On** option.
 - c. Select **All Error** for the error handling setting. This will halt the system if any hardware error is found. If the **No Error** option is retained, the system will continue booting even if any hardware error exists such as the absence of a keyboard or mouse.
 - d. Access the **Exit** page and verify that the **Exit Saving Changes** option is selected.
 - e. To confirm and exit, press **Enter**.
2. Check the boot sequence.
 - a. Access BIOS according to the manufacturer's instruction.
 - b. Access the Boot menu.
 - c. Order the devices in the desired boot sequence using the (+) or (-) keys to move the sequence up or down. The system will boot from the device that is at the top of the boot sequence.
 - d. Save the setting and exit the BIOS screen.

BIOS Variations

While setting the boot sequence, the BIOS settings and options will vary according to the BIOS version, type, and the system. For example, in some BIOS, it will be the Boot Sequence, whereas in others it may be the Boot Order or Startup Sequence. Similarly, most options—right from accessing the BIOS screen to the various configuration settings—will vary. You can either read through the vendor manual or follow the instructions that appear on the BIOS screen to perform the desired task.

Bootable Devices

The common bootable devices include the following:

- External Storage Device
- IDE Hard Drive
- ATAPI CD-ROM
- Other Boot Device

Procedure Reference: Enable or Disable Integrated Peripherals

To enable or disable integrated peripherals such as serial ports, parallel ports, modems, and sound cards:

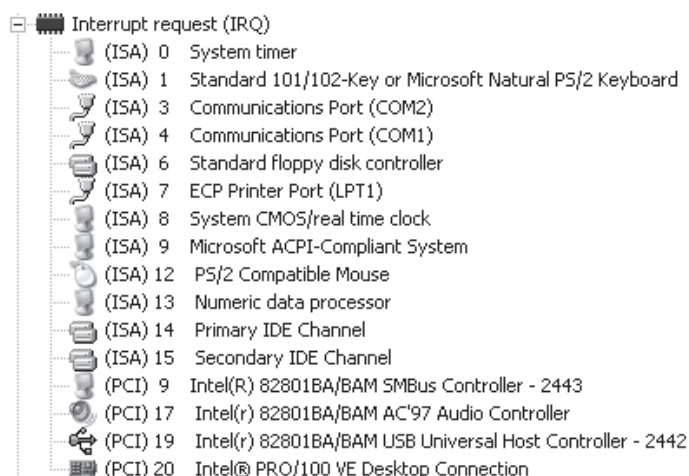
1. Access BIOS according to the manufacturer's instruction.
2. Access the **Advanced** menu.
3. Select the **I/O Device Configuration** option and press **Enter**.
4. Select the desired peripheral you want to enable or disable and press **Enter**.
 - To enable the peripheral, select the desired Interrupt/IRQ values and press **Enter**.
 - To disable the peripheral in case of an IRQ/IO conflict, select the **Disabled** option.
5. To return to the **Advanced** menu, press **Esc**.
6. Save the setting and exit BIOS.

Correct Settings for IRQ, DMA, and I/O Addresses

In the case of an IRQ/IO conflict with devices such as modem and sound cards, you can change the setting for these devices. After selecting the desired peripheral in the **Advanced Menu** screen, press **Enter** to view the options and select the IRQ/IO options desired for the peripheral.

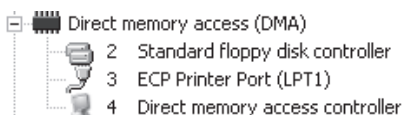
Common IRQ Settings

Some of the typical Interrupt Request (IRQ) settings are shown in the figure.



Common DMA Settings

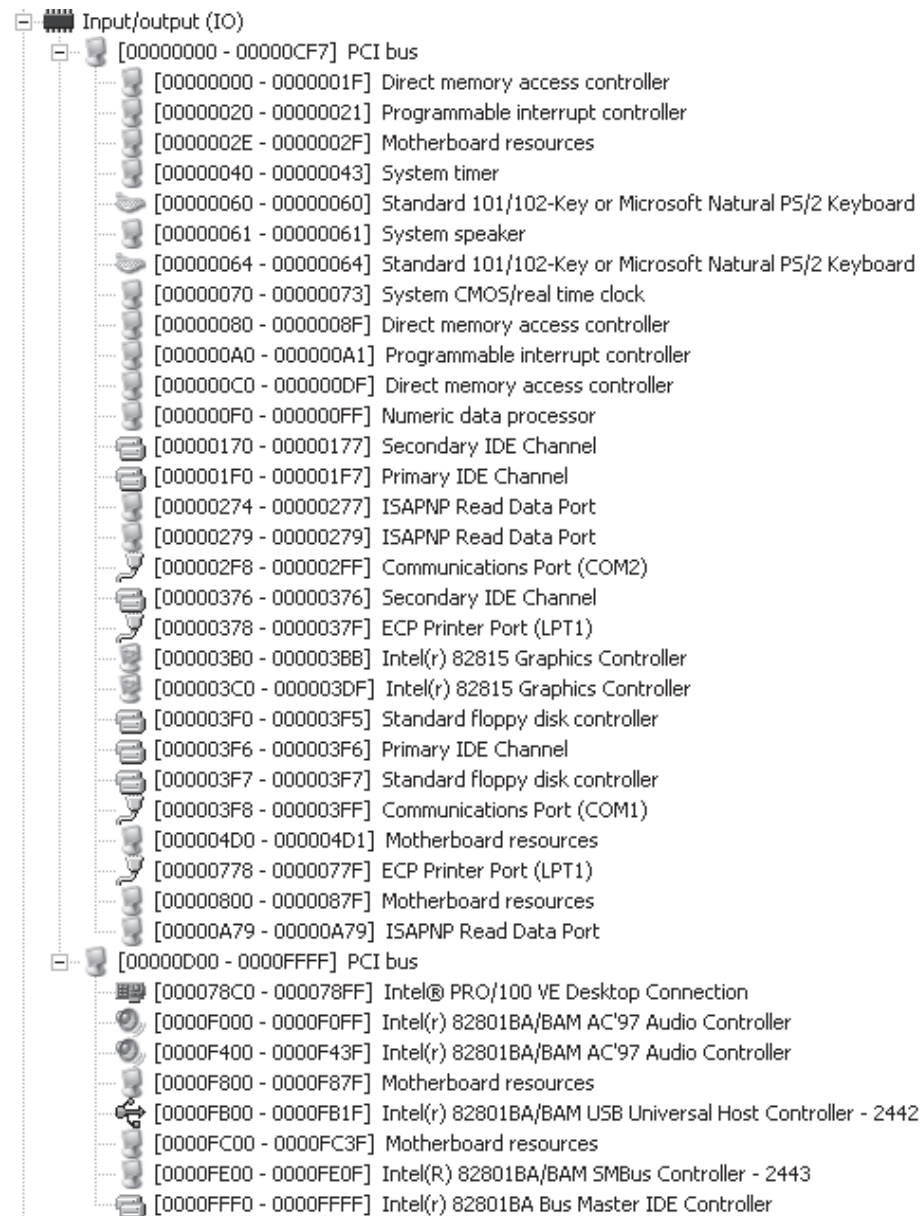
Some of the typical Direct Memory Access (DMA) settings are shown in the figure.



Common I/O Settings

Some of the typical Input/Output (I/O) settings are shown in the figure.

LESSON 17



DISCOVERY ACTIVITY 17-1

Preparing to Install Linux

Scenario:

You are a system administrator for OGC, who had been considering a switch to Linux. The final approval to implement Linux across the organization has been granted and your manager, Peter, asked you to handle the company-wide implementation of Linux. Peter would first like you to develop a procedure to help prepare all systems for a Linux installation.

1. **What is the default boot loader in new versions of Red Hat Enterprise Linux?**
 - a) LILO
 - b) GRUB
 - c) System Commander

2. **True or False? FIPS is used to resize FAT partitions.**
☐ True
☐ False

3. **When is it the best time to gather information about your Linux system?**
 - a) Just after installing Linux.
 - b) During the Linux installation.
 - c) Before installing Linux.
 - d) You do not have to gather system information.

TOPIC B

Identify the Phases of the Linux Boot Sequence

In the last topic, you identified Linux compatible hardware and types of installation techniques. To understand how Linux is loaded on to your system, you need to learn about the boot process. In this topic, you will identify phases of the Linux boot sequence and its components.

The boot process is the most important process in system startup, and it is essential for proper loading of the operating system and all its applications. While installing Linux on multiple computers, it is important that you have sound knowledge of the boot process because it will help you identify and troubleshoot any issues related to system startup or the operating system.

Boot Loaders

Definition:

A *boot loader* is a program that loads the kernel from the hard drive, or boot disk, and then starts the operating system. It is also referred to as the boot manager. Although boot loaders can load more than one operating system into the computer's memory, the user needs to select the desired operating system. Boot loaders interact with BIOS and utilize subroutines to load the operating system. In addition, they protect the boot process with a password.

Example:

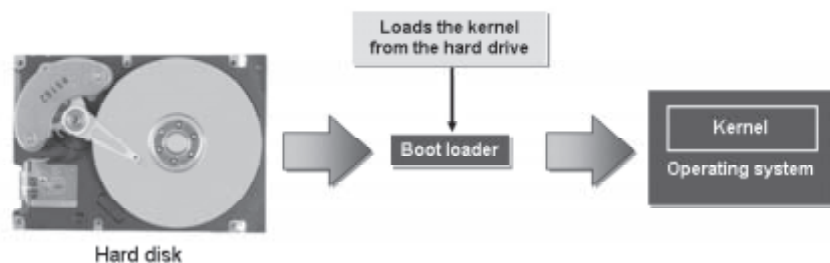


Figure 17-3: The function of a boot loader.

Boot Loader Components

The boot loader uses three main components that work together to systematically load the operating system in stages.

Component	Description
Boot sector program	It is the first component of the boot loader. It is loaded by BIOS on startup and has a fixed size of 512 bytes. Its main function is to load the second stage boot loader; however, it can also load another sector or a kernel.

Component	Description
Second stage boot loader	It loads the operating system and contains a kernel loader.
Boot loader installer	It controls the installation of disk sectors and can be run only when booting from a disk. It coordinates the activities of the boot sector and the boot loader.

Types of Boot Loaders

There are different types of boot loaders in Linux. Some of the boot loaders are described in the following table.

Boot Loader	Description
<i>GRUB</i>	A popular Linux boot loader that allows you to place specific instructions in MBR.
<i>ELILO</i>	A boot loader for Unified Extensible Firmware Interface (UEFI) machines. It supports flexible local booting from a FAT-32 filesystem and a wide variety of boot options via network booting over DHCP/TFTP.
<i>System Commander</i>	A third-party boot loader that can also be used as a boot manager. This utility enables you to control the environment you boot into. It has a full-featured boot manager and partitioning software.
<i>SysLinux</i>	An MS-DOS program that is sometimes used to simplify a first-time installation of Linux and for creating a rescue boot disc.

GRUB Loading Order

GRUB loads in the following order: the primary boot loader is loaded first, followed by the secondary boot loader and, finally, the operating system. After receiving the correct instructions for the operating system to start, GRUB locates the boot file and hands off control of the machine to that operating system.

UEFI

Earlier known as Extensible Firmware Interface (EFI), UEFI specifies an interface that operates between the operating system and the platform firmware. It is an alternative to BIOS for initiating a system, but does not completely replace BIOS.

GRUB 2

GRUB 2 is the newest version of the GRand Unified Bootloader. The original version of GRUB is now referred to as GRUB Legacy. Both versions are in use in Linux distributions.

What's New in GRUB 2

GRUB is the GRand Unified Bootloader program that loads operating system kernels. The bootloader known as GRUB is now called GRUB Legacy and is no longer actively developed. GRUB 2 is the new GRUB version being adopted by Linux distributions. However, GRUB 2 is more than simply a newer version of GRUB; it is a complete redesign and rewrite of the GRUB system. GRUB 2 offers administrators more control over the boot process, boot devices and boot behavior. There are changes to configuration files, filenames and file locations in GRUB 2. Some of the major changes are outlined in the following table.

GRUB Legacy	GRUB 2
/boot/grub/menu.lst or /boot/grub/grub.conf	/boot/grub/grub.cfg
Menu displayed during boot	No menu displayed during boot. To display the menu during boot, press Shift or Esc.
First partition number is 0	First partition number is 1
Manual update of menu.lst to include Linux kernels	Menu list of available Linux kernels auto-generated by running update-grub
No Loadable Modules	Loadable Modules
Menu <i>title</i>	Menu <i>menuentry</i>
Directly editable menu.lst file	Indirectly editable grub.cfg. Edit the grub.cfg file by editing entries in the /etc/default/grub file and files in the /etc/grub.d directory.


The Boot Process

The *boot process* is repeated each time your computer is started by loading the operating system from the hard drive. It involves a series of sequential steps that can be divided into BIOS initialization, boot loader, kernel and init initialization, and boot scripts.

The boot process consists of the following steps:

1. The processor checks for the BIOS program and executes it.
2. BIOS checks for peripherals, such as floppy disk drives, CD-ROMs, and the hard disk, for bootable media. It locates a valid device to boot the system.
3. BIOS loads the primary boot loader from the MBR into memory. The boot loader is a program that contains instructions required to boot a machine. It also loads the partition table along with it.
4. The user is prompted with a graphical screen that displays the different operating systems available in the system to boot from. The user should select an operating system and press **Enter** to boot the system. If the user does not respond, then the default operating system will be booted.
5. The boot loader determines the kernel and locates the corresponding kernel binary. It then uploads the respective `initrd` image into memory and transfers control of the boot process to the kernel.

6. The kernel configures the available hardware, including processors, I/O subsystems, and storage devices. It decompresses the `initrd` image and mounts it to load the necessary drivers. If the system implemented any virtual devices, such as LVM or software RAID, then they are initialized. The components configured by the kernel will be displayed one by one on the screen.
7. The kernel mounts the root partition and releases unused memory. To set up the user environment, the `init` program is executed.
8. The `init` program searches for the `inittab` file, which contains details of the runlevel, that has to be started. It sets the environment path, checks the filesystem, initializes the serial ports, and runs background processes for the runlevel.
9. If graphical mode is selected, then `xdm` or `kdm` is started and the login window is displayed on the screen.
10. The user enters the user name and password to log in to the system.
11. The system authenticates the user. If the user is valid, then the profile, the `.login`, the `.bash_login`, and the `.bash_profile` files are executed. The shell is started and the system is ready for the user to work on.

 `xdm` refers to the X Window Desktop Manager. Users who utilize GNOME or KDE, use either `gdm` or `kdm`, respectively. In RHEL 5.3, `gdm` is the default desktop manager.

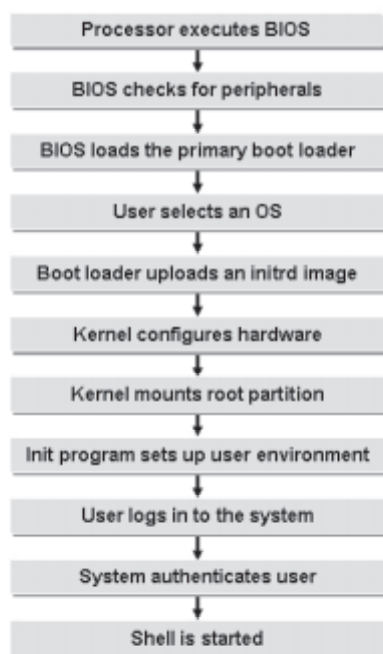



Figure 17-4: Stages in the boot process.

Superblocks

Definition:

A *superblock*, often called `sb`, is a data structure that is stored on a disk and contains control information for a filesystem. Linux partitions are discussed in terms of blocks. A superblock comprises the first 512 bytes of a partition. It contains information about the block size used by the filesystem, the location of the root directory, and the time it was last checked.

 Each partition on a disk is identified by a number. The number 1, is assigned to the first partition, number 2, to the second partition, and so on.

Example:



Figure 17-5: A superblock on a hard disk.

Sectors

Definition:

A *sector* is the smallest unit of storage read from or written onto a disk. A sector stores 512 bytes of data by default. A collection of sectors is called a track. The number of sectors in a track may vary, and so does their capacity to hold data. The size of a sector can be altered when formatting the hard disk.

Example:

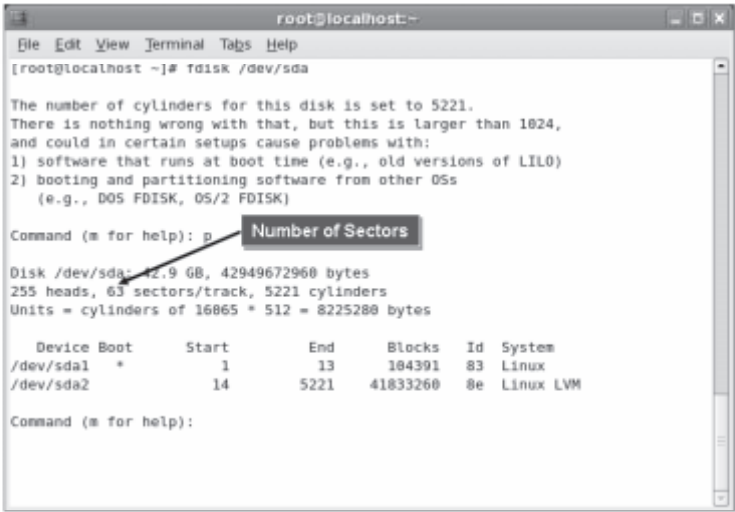
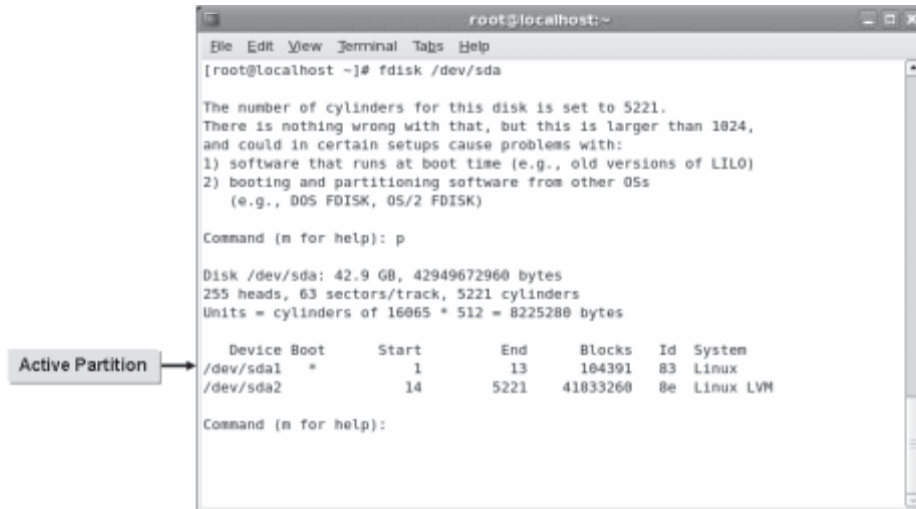


Figure 17-6: A hard disk showing sectors and tracks.

MBR

Definition:

Master Boot Record (MBR) is the first physical sector on a hard drive. It contains the code used for loading the operating system or boot loader into memory. It also contains the partition table of the hard drive. MBR helps determine the partition that is currently active.

Example:


```

root@localhost:~
File Edit View Terminal Tabs Help
[root@localhost ~]# fdisk /dev/sda

The number of cylinders for this disk is set to 5221.
There is nothing wrong with that, but this is larger than 1024,
and could in certain setups cause problems with:
 1) software that runs at boot time (e.g., old versions of LILO)
 2) booting and partitioning software from other OSs
   (e.g., DOS FDISK, OS/2 FDISK)

Command (m for help): p

Disk /dev/sda: 42.9 GB, 42949672960 bytes
255 heads, 63 sectors/track, 5221 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1  *         1           13      104391   83  Linux
/dev/sda2                14        5221     41833260  8e  Linux LVM

Command (m for help):

```

Figure 17-7: A hard disk showing MBR and the partition table loaded by it.

ACTIVITY 17-2

Discussing the Boot Process

Scenario:

As a junior administrator, you have instructions to get acquainted with the boot sequence components because understanding how they work will help you troubleshoot any issues that may arise when loading the operating systems onto machines for new users.

1. What enables you to choose the operating system to load from the hard disk?
 - a) The boot loader
 - b) MBR
 - c) The number of tracks on the hard disk
 - d) BIOS
2. What is true of MBR? Select all that apply.
 - a) MBR contains the partition tables.
 - b) MBR contains a number of sectors.
 - c) MBR contains the code to load the operating system into memory.
 - d) MBR determines the boot device settings.
 - e) MBR determines the currently active partition.

3. True or False? The boot loader installer contains a kernel loader.

- ___ True
___ False

TOPIC C

Configure GRUB

In the last topic, you discussed the boot sequence. To manage the boot process, you must understand how to use and configure the components involved in it. By configuring GRUB, you can modify the system to run it according to your requirements. In this topic, you will configure the GRUB boot loader and understand its functions.

As a Linux administrator, you may be assigned the task of running multiple operating systems on the same system. In such a case, you must know how to add new kernels and boot the correct operating system. To accomplish this task, you should know about GRUB and how to configure it.

GRUB

Definition:

GRand Unified Bootloader (GRUB) is a program that is used to install a boot loader in MBR. GRUB allows you to place specific instructions in MBR to load a GRUB menu or environment command. This enables you to start the operating system of your choice, pass instructions to the kernel when booting, or check for system parameters before booting.

Example:

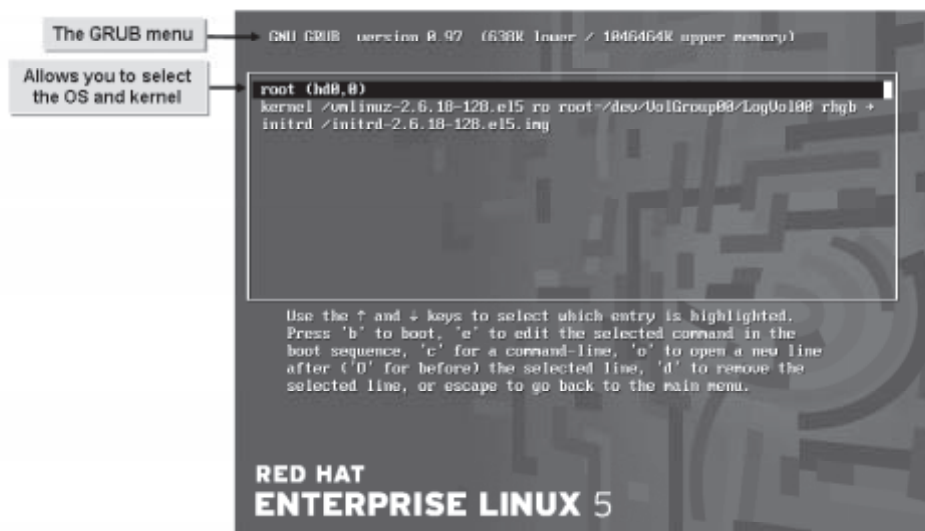


Figure 17-8: The grub boot loader menu screen with its various functions.

The grub.conf File

The `grub.conf` file found in the `/boot/grub` directory is the configuration file for the GRUB boot manager. It contains various configuration options for configuring and troubleshooting the boot manager.

Option	Enables You To
<code>default={number}</code>	Specify the default booting kernel number if multiple kernel images are found.
<code>timeout={number}</code>	Specify the time limit for the login screen to be displayed.
<code>splashimage=(hdx,y)/grub/{image location}</code>	Specify the location of the login screen image.
<code>title {user desired name}</code>	Specify a title to differentiate between the kernel images in the login screen.
<code>root (hdx,y)</code>	Specify the location of MBR.
<code>kernel {location} [option]</code>	Specify the location of the kernel.
<code>initrd {kernel image}</code>	Specify the location of the kernel image.

```

root@localhost:~
File Edit View Terminal Tabs Help
[root@localhost ~]# cat /boot/grub/grub.conf
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE: You have a /boot partition. This means that
#           all kernel and initrd paths are relative to /boot/, eg.
#           root (hd0,0)
#           kernel /vmlinuz-version ro root=/dev/VolGroup00/LogVol00
#           initrd /initrd-version.img
#boot=/dev/sda
default=0
timeout=5
splashimage=(hd0,0)/grub/splash.xpm.gz
hiddenmenu
title Red Hat Enterprise Linux Server (2.6.18-128.el5)
    root (hd0,0)
    kernel /vmlinuz-2.6.18-128.el5 ro root=/dev/VolGroup00/LogVol00 rhgb qui
et
    initrd /initrd-2.6.18-128.el5.img
[root@localhost ~]#
  
```

Figure 17-9: The `grub.conf` file that is used to configure the GRUB boot manager.

The GRUB Menu Configuration File

The configuration file, `/boot/grub/grub.conf`, is used to create a list of operating systems to boot from. This allows a user to select a group of commands to execute, which will launch the desired operating system.

The menu.lst File

The `menu.lst` file is a GRUB configuration file that lists all the kernels available on the system along with their partition numbers, boot information, and details of which kernel is booted. The `menu.lst` file is stored in the `/boot/grub/` directory.

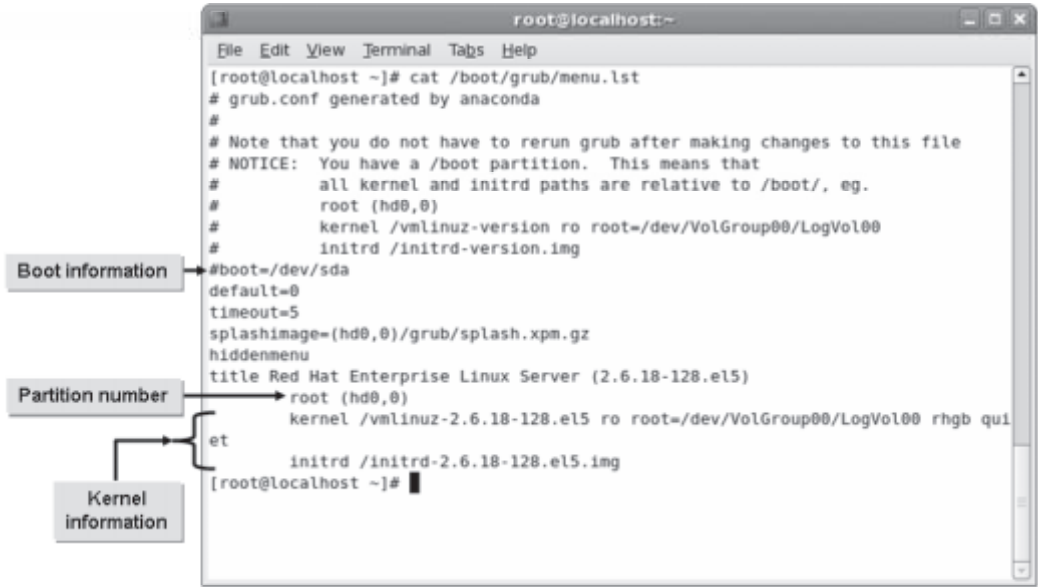


Figure 17-10: The menu.lst file displaying the system’s kernel details.

GRUB Commands

GRUB commands enable a user to configure and modify the GRUB settings in each runlevel, based on user requirements. GRUB commands are categorized as general and CLI commands.

General Command	Enables You To
bootp	Use the BOOTP protocol to initialize a network device.
device	Create a disk image and specify a file as a BIOS drive. This command is also used to troubleshoot GRUB in case of drive errors.
dhcp	Use the DHCP protocol to initialize a network device.
password	Set a password for the menu files. The locked files will not have the edit property set to them.
ifconfig	Configure a network manually. The gateway, IP address, subnet mask, and server address can be configured using this command.
terminal	Specify the terminal settings. Serial ports can be used only if this command is specified.
serial	Configure settings for various serial devices and serial ports.

CLI Command	Enables You To
boot	Load the operating system into the computer from the CLI.

CLI Command	Enables You To
<code>cat {file name}</code>	Display the content of a file.
<code>find</code>	Search for a file.
<code>setup</code>	Install and configure various services such as authentication, firewalls, and system services.
<code>install</code>	Install GRUB and other utilities.
<code>kernel</code>	Load a kernel boot image.
<code>lmodule</code>	Load a kernel module.
<code>halt</code>	Shutdown your system.
<code>reboot</code>	Reboot your system.
<code>exit</code>	Exit from the GRUB shell.



Figure 17-11: The commands that can be executed at the GRUB prompt.

GRUB Menu-Specific Commands

Menu-specific commands are used to configure GRUB from the configuration file. They can be enabled in the global section of the `grub.conf` configuration file.

Command	Enables You To
<code>default</code>	Set the default entry for the entry number NUM, which is used by GRUB in case of boot entry errors.
<code>fallback</code>	Set the fallback entry, allowing GRUB to override any errors in the boot entry.
<code>hiddenmenu</code>	Hide the menu control from a user at the control terminal. This does not affect the boot entry.

Command	Enables You To
<code>timeout</code>	Set the timeout value before booting into the default boot entry. The <code>hiddenmenu</code> command can be disabled here by pressing Esc before timeout elapses.
<code>title</code>	Start a new boot entry, which is displayed on the menu interface.

How to Configure GRUB

Procedure Reference: Configure the GRUB Boot Loader

To configure the GRUB boot loader:

1. Log in as root in the CLI.
2. To open the `grub.conf` file, enter `vi /boot/grub/grub.conf`.



You can also use the softlink `/boot/grub/menu.lst` file to configure the GRUB boot manager.

3. Make the necessary changes to specify alternative boot locations and backup options.
4. Save and close the file.

Procedure Reference: Protect GRUB with a Password

To protect GRUB with a password:

1. Log in as root in the CLI.
2. To create an MD5 encrypted password, enter `grub-md5-crypt`.
3. To navigate to the `/boot/grub` directory, enter `cd /boot/grub`.
4. To open the `grub.conf` file, enter `vi grub.conf`.
5. To switch to insert mode, press **I**.
6. To specify your password, on a new line below the **hiddenmenu** option, type `password --md5`.
7. Save and close the file.

Procedure Reference: Install GRUB as the Boot Loader

To install GRUB as the boot loader:

1. Log in as root in the CLI.
2. To identify the boot device of the system, enter `cat /boot/grub/device.map`.
3. To install the GRUB boot loader, enter `grub-install {boot device}`.
4. To check if the system boots with the specified boot loader, enter `reboot`.

Procedure Reference: Set Up GRUB Manually

To set up GRUB manually:

1. Log in as root.
2. To open the GRUB shell, at the command prompt, enter `grub`.
3. Enter `root (boot device node, partition)`.
4. Enter `setup (boot device node, partition)`.
5. To close the GRUB shell, enter `quit`.
6. To reboot the system, enter `reboot`.

Procedure Reference: Boot from Menu Editing Mode

To boot from menu editing mode:

1. Start the system.
2. On the GRUB graphical splash screen, press **Esc**.
3. To enter menu editing mode, select an entry and press **E**.
 - To edit a line, select the line and press **E**.
 - To delete a line, select the line and press **D**.
 - To add a line, select the line and press **O**.
 - To open the GRUB shell, select a line and press **C**.
4. To boot the system, press **B**.

Procedure Reference: Set the Correct Hardware ID Number for Different Devices

To set the correct hardware ID number for different devices:

1. Start the system and press the appropriate keys to access the SCSI BIOS utility screen.
2. In the **Options** section, select the **Configure/View Host Adapter Settings** option and press **Enter**.
3. Access the **Boot Device** option and press **Enter**.
4. On the **Boot Device Configuration** screen, press **Enter** and select the desired device ID from which you want to boot and press **Enter**.
5. To go to the main screen, press **Esc** three times.
6. Save the settings and exit BIOS.

ACTIVITY 17-3

Configuring GRUB

Before You Begin:


- 1. On srvB, log in as root in the GUI.
- 2. Switch to the CLI terminal.

Scenario:

The system administrator is receiving many complaints from users that their systems are not booting properly. As a junior administrator, you are assigned the task of troubleshooting the systems. You find that the boot loader is not installed properly, and that someone has modified the settings in the boot loader because there is no password protection. You decide to reinstall GRUB and protect it with a password.

These are your login details:

- Your login id is root.
- Your password is p@ssw0rd.

What You Do	How You Do It
1. Install the GRUB boot manager.	<div>a. Log in as root in the CLI.</div> <div>b. To install GRUB, enter grub-install /dev/hda</div> <div>c. Verify that the “Installation finished. No error reported” message is displayed. This indicates that GRUB has been installed successfully.</div>
2. Generate an MD5 encrypted password for GRUB.	<div>a. To generate an MD5 password for GRUB, enter grub-md5-crypt</div> <div>b. At the Password prompt, enter p@ssw0rd</div> <div>c. At the Retype password prompt, enter p@ssw0rd</div> <div>d. Observe the MD5 password that is generated.</div> <div> This MD5 password will be used in the activity to protect GRUB with a password.</div>

3. Enable password protection for GRUB.
 - a. To navigate to the `/boot/grub` directory, enter **`cd /boot/grub`**
 - b. To open the `grub.conf` file, enter **`vi grub.conf`**
 - c. To go to the **`hiddenmenu`** line, enter **`/hid`**
 - d. To switch to insert mode and move to a new line, press **`O`**.
 - e. On the line below the **`hiddenmenu`** option, type **`password --md5 password`** In the password section, students must type the MD5 password that they have generated.
 - f. To switch to command mode, press **`Esc`**.
 - g. Save and close the file.
-
4. Check whether password protection is enabled for GRUB.
 - a. To restart the system, enter **`reboot`**
 - b. On the **GRUB** graphical splash screen, press **`A`**.
 Unless you specify the password, you will not be able to edit the GRUB from the splash screen. Thus, password protection is enabled for the GRUB boot loader.
 - c. To enter the password, press **`P`**.
 - d. At the **Password** prompt, enter **`p@ssw0rd`**
 - e. To edit the GRUB configuration, press **`E`**.
 - f. To boot with the default setup, press **`B`**.
-

TOPIC D

Install the Operating System

You may have installed various operating systems previously. However, installation techniques do not apply universally to all operating systems. With a clear understanding of the boot process, you will be prepared to begin the installation of Linux. In this topic, you will install Linux on a computer after ensuring that the computer is suitable to host it.

Installation is perhaps the most important aspect in the Linux operating system. It involves many major tasks such as creating and configuring partitions and devices. Also, Linux can be installed in different ways. As a Linux administrator, you may be required to install and reinstall Linux on a number of systems. Knowing how to administer Linux installation will enable you to utilize the potential of the features packed into Linux to the optimum.

How to Install the Operating System

Procedure Reference: Install Linux from a CD-ROM

To install Linux from a CD-ROM:

1. At the boot prompt, choose the mode of installation either as text or graphical mode.
2. If necessary, check the boot media and start the installation.
3. To begin the installation, click **Next**.
4. Choose the desired language.
5. Choose the desired keyboard type.
6. Enter the installation number and click **OK**.
7. A warning message will be displayed if you are using a new hard disk; click **Yes** to continue.
8. From the partition layout drop-down list, select the desired partition layout and click **Next**.
9. If a warning message is displayed, click **Yes** to continue.
10. If necessary, review the partition table and click **Next**.
11. On the boot loader installation page, choose the type of boot loader and its location and then click **Next**.
12. On the network configuration page, configure the network and click **Next**.
13. Select the desired time zone for the machine and click **Next**.
14. Enter the root password and click **Next**.
15. Accept the default package list or select **Customize now** and click **Next**.
16. Select the necessary package and click **Next**.
17. On the installation complete page, click **Reboot** to finish the installation and reboot the system.

Procedure Reference: Install Linux on a Network

To install Linux on a network:

1. To view the boot medium options, at the boot prompt, enter `linux askmethod`
2. Select the appropriate network installation medium and press **Enter**.
3. Choose the desired language.
4. Choose the desired keyboard type.
5. Choose the type of installation method.
6. Configure the network settings.
7. Specify the remote install server information.
8. If necessary, check the boot media and start the installation.
9. Click **Next** to begin the installation.
10. Enter the installation number and click **OK**.
11. A warning message will be displayed if you are using a new hard disk; click **Yes** to continue.
12. From the partition layout drop-down list, select the desired partition layout and click **Next**.
13. If a warning message is displayed, click **Yes** to continue.
14. If necessary, review the partition table and click **Next**.
15. On the boot loader installation page, choose the type of boot loader and its location and then click **Next**.
16. On the network configuration page, configure the network and click **Next**.
17. Select the desired time zone for the machine and click **Next**.
18. Enter the root password and click **Next**.
19. Accept the default package list or select **Customize now** and click **Next**.
20. Select the necessary package and click **Next**.
21. On the installation complete page, click **Reboot** to finish the installation and reboot the system.

Procedure Reference: Configure the Post-Installation Settings

To configure the post-installation settings:

1. On the post installation welcome screen, click **Forward**.
2. Accept the license agreement and click **Forward**.
3. If necessary, customize the **Firewall** settings and click **Forward**.
4. If necessary, customize the **SELinux** settings and click **Forward**.
5. If necessary, enable **kdump** and click **Forward**.
6. If necessary, customize the **Date and Time** settings and click **Forward**.
7. Set up software updates with RHN and click **Forward**.

8. Create a user and click **Forward**.
9. If necessary, customize the sound card settings and click **Forward**.
10. If necessary, install software from additional CDs.
11. Click **Finish** to complete the installation.
12. Log in to the system using the user name and password.

Procedure Reference: Access the Network Installation Server

To access the network installation server:

1. Log in as root.
2. Insert the installation CD into the CD-ROM and mount it using the command `mount /dev/cdrom /{mount point}`.
3. To copy the installation image into the destination folder, enter `cp -R /{mount point}/* /{destination directory}/`.
4. Replace the CD with the next installation CD and perform steps 2 and 3.
5. Configure the server to be used during the remote installation.
 - a. Configure the NFS server for network installation.
 1. To open the exports file, enter `vi /etc/exports`.
 2. To specify the destination directory for obtaining installation files, type `/ {destination directory} [options]`.
 3. Save and close the file.
 4. To start the NFS server, enter `service nfs start`.
 5. To export the directory, enter `exportfs -r`.
 - b. Configure the FTP server for network installation.
 1. Ensure that `/ {destination directory}` is `/var/ftp/pub` for FTP-based installation.
 2. To specify the destination directory for obtaining installation files, type `/ {destination directory} [options]`.
 3. Save and close the file.
 4. To start the FTP server, enter `service vsftpd start`.
 - c. Configure the HTTP server for network installation.
 1. Ensure that `/ {destination directory}` is `/var/www/html` for HTTP-based installation.
 2. To specify the destination directory for obtaining installation files, type `/ {destination directory} [options]`.
 3. Save and close the file.
 4. To start the httpd server, enter `service httpd start`.

Procedure Reference: Create a Boot Media

To create a boot media:

1. Log in as root.

2. Create a boot media.
 - a. Create a boot CD.
 1. To copy the boot image to the specified location, at the command prompt, enter `cp /media/images/boot.iso {destination directory}`.
 2. To navigate to that location, enter `cd {destination directory}`.
 3. To create the boot CD, enter `cdrecord -v boot.iso`.
 - b. Create a boot USB drive.
 1. To redirect the bootdisk.img content to where the USB device node is located, at the command prompt, enter `cat /media/images/bootdisk.img > /dev/{device name}{device number}`.

ACTIVITY 17-4

Installing Linux

Before You Begin:

1. On srvB, the GUI login screen is displayed.
2. Insert the Red Hat Enterprise Linux CD 1 in the CD-ROM drive and reboot the system from the CD-ROM.

Scenario:

A Linux system needs to be allocated to a new employee of your organization. You have been assigned the task of installing the Linux operating system and configuring the basic network settings to connect to the organization's network.

LESSON 17

What You Do

1. Initiate the Red Hat Enterprise Linux 5 installation process for a server system.



Ensure that the Red Hat Enterprise Linux CD 1 is inserted in the CD-ROM drive and boot the system from the CD-ROM.

How You Do It

- a. To install Linux in graphical mode, at the boot prompt, press **Enter**.
 - b. To skip the media test and start the installation process, on the **Welcome to Red Hat Enterprise Linux Server** page, in the **CD Found** dialog box, press **Tab** and then press **Enter**.
 - c. On the Red Hat Enterprise Linux 5 page, click **Next**.
 - d. On the Language Selection page, in the language selection list box, verify that the **English (English)** option is selected and then click **Next**.
 - e. On the Keyboard Configuration page, verify that the **U.S. English** option in the Keyboard section is selected and then click **Next**.
 - f. In the **Installation Number** dialog box, enter the installation number and click **OK**.
 - g. On the Installation Option page, verify that the **Install Red Hat Enterprise Linux Server** option is selected and click **Next**.
-
2. Partition the hard disk manually.
 - a. Verify that the **Remove linux partitions on selected drives and create default layout** option is selected and click **Next**.
 - b. In the **Warning** message box, click **Yes**.
-


3. Set the network configuration.
 - a. In the **Network Devices** section, click **Edit**.
 - b. In the **Edit Interface** dialog box, in the **Enable IPv4 support** section, select the **Manual configuration** option and uncheck the **Enable IPv6 support** check box.
 - c. In the **IPv4** section, in the **Address** text box, type **192.168.0.< number>** and then press **Tab**.
 - d. In the **Prefix (Netmask)** text box, type **255.255.255.0** and click **OK**.
 - e. On the Network Configuration page, verify that in the **Hostname** section, in the **manually** text box, the hostname **localhost.localdomain** is displayed and then click **Next**.
 - f. To proceed with the installation without specifying the IP address of the gateway system, in the **Error With Data** message box, click **Continue**.
 - g. To proceed with the installation without specifying the IP address of the primary DNS system, in the **Error With Data** message box, click **Continue**.

 4. Set the time zone and root password.
 - a. On the Time Zone Selection page, in the Location section, verify that the **America/New_York** option is selected and then click **Next**.
 - b. On the Set Root Password page, in the **Root Password** text box, type **p@ssw0rd** and press **Tab**.
 - c. In the **Confirm** text box, type **p@ssw0rd** and click **Next**.
-

LESSON 17

5. Select the required software packages for the system.
 - a. On the Software Selection page, in the include support section, check the **Software Development** and **Web server** check boxes. Uncheck the **Virtualization** check box and click **Next**.
 - b. In the Customize section, select the **Customize now** option and then click **Next**.
 - c. On the Package Selection page, in the first list box, verify that the **Desktop Environments** option is selected and in the adjacent list box, check the **KDE (K Desktop Environment)** check box.
 - d. In the first list box, select the **Servers** option, and in the adjacent list box, check the **DNS Name Server**, **FTP Server**, and **Network Servers** check boxes.
 - e. In the first list box, select the **Base System** option, and in the adjacent list box, check the **System Tools** check box and then click **Next**.

6. Install the software packages.
 - a. On the Begin Installation page, click **Next**.
 - b. In the **Required Install Media** message box, click **Continue**.

 The required set of CDs, as displayed on the Required Install Media dialog box, must be kept ready before proceeding with the installation process.
 - c. When prompted, insert Red Hat Linux CD-02, CD-03, and CD-04 into the CD drive.
 - d. On the Congratulations page, click **Reboot**.

7. Configure the post installation settings.
 - a. On the **Welcome** page, click **Forward**.
 - b. On the **License Agreement** page, verify that the **Yes, I agree to the License Agreement** option is selected and then click **Forward**.
 - c. On the **Firewall** page, from the **Firewall** drop-down list, select **Disabled** and then click **Forward**.
 - d. In the confirmation message box, click **Yes**.
 - e. On the **SELinux** page, from the **SELinux Setting** drop-down list, select **Disabled** and then click **Forward**.
 - f. In the confirmation message box, click **Yes**.
 - g. On the **Kdump** page, click **Forward**.
 - h. On the **Date and Time** page, verify that the date and time is set to the current date and time and then click **Forward**.
 - i. On the **Set Up Software Updates** page, select the **No, I prefer to register at a later time** option and click **Forward**.
 - j. In the Red Hat Network connection dialog box, click **No thanks, I'll connect later**.
 - k. On the **Finish Updates Setup** page, click **Forward**.
 - l. On the **Create User** page, click **Forward**.
 - m. In the confirmation message box, click **Continue**.
 - n. On the **Sound Card** page, click **Forward**.
 - o. On the **Additional CDs** page, click **Finish**.
 - p. To reboot the system, in the confirmation message box, click **OK**.
-

TOPIC E

Perform Post-Installation Tasks

In the last topic, you successfully installed Linux. Now, you need to begin using the operating system. In this topic, you will perform post-installation tasks.

Before working with your new Linux system, you need to perform certain basic tasks. To begin with, if you want to use the GUI environment, you must configure X Windows. Secondly, you must document your settings. Documentation is the key to solving future problems, getting equipment upgrades, and preventing financial losses from network troubles. Documenting changes to setups, configurations, topologies, and histories can help you troubleshoot problems that arise later.

The X Windows Configuration

X Windows, also known as *X* or *X11*, is a client/server, multiuser system that resides on top of the operating system. The X Window system configuration option provides you with a choice of using a graphical or text-based interface. The primary configuration file defines hardware devices and other critical components of the X server environment. Configuration options include monitor, video card, keyboard, pointing device, and many more.

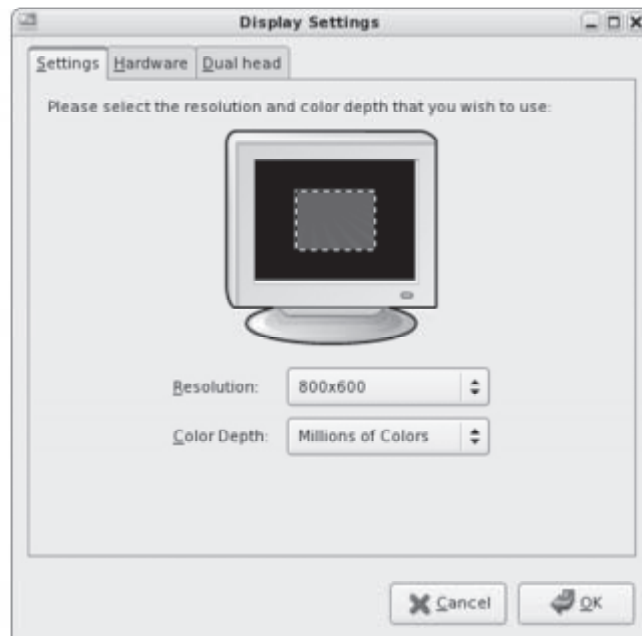


Figure 17-12: The Display Settings dialog box that is used to configure X Windows.

Red Hat Runlevel

If you configure the X Window system during the Red Hat Linux installation program, you have the option of choosing a graphical or text login screen. If you choose a text login screen, you will be operating in runlevel 3. If you choose a graphical login screen, you will be operating in runlevel 5.

Virtual Desktops

There will be times when a user needs to have multiple windows open on their desktop. Typically, to help manage the need to go between many different programs running simultaneously, users would do one of three things:

- Leave all windows open, which may result in a cluttered desktop.
- Minimize those windows that are not needed and use the taskbar or press **Alt+Tab** to switch between them. This approach could still be a bit confusing.
- Or, use virtual desktops.

The default configuration provides two or four desktops depending on the distribution. For example, Ubuntu provides two desktops by default and RHEL provides four. Users can switch between the virtual desktops by clicking one of the desktop buttons on the panel at the bottom of the desktop screen.

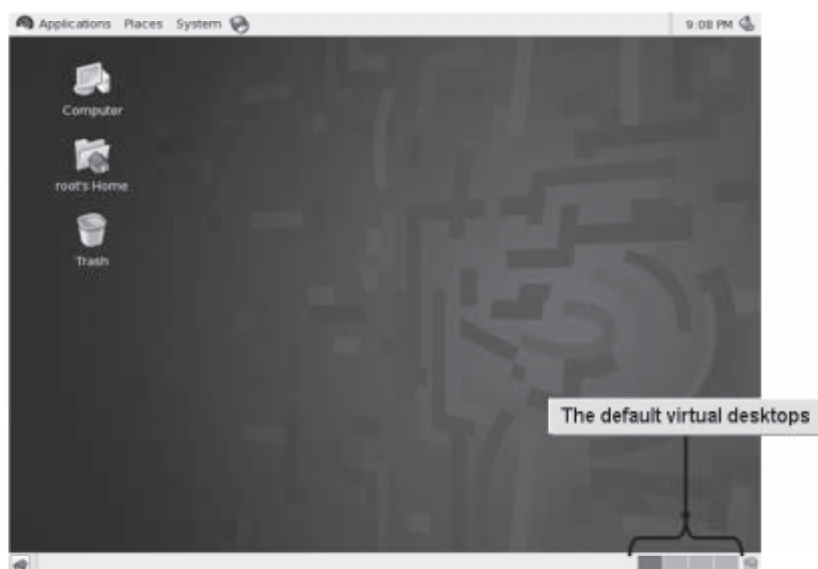


Figure 17-13: Virtual desktop buttons on the panel.

Documentation

Sufficient and proper documentation of setups, configurations, topologies, and histories can prove valuable while troubleshooting. This includes documenting the hardware and software components installed, why and when they were installed, by whom, and other important and specific information.

Include Log File Information

Check the log files:

- /var/log/messages
- /var/log/dmesg
- /tmp/install

These files contain information captured during the installation. You may want to include hard copies of these files in your installation documentation.

How to Perform Post-Installation Tasks

Procedure Reference: Configure X Windows

- To configure X Windows:
1. Log in to GNOME.
 2. Choose **Applications→System Settings→Display**.
 3. If necessary, adjust the **Display** settings.
 - Resolution
 - Color Depth
 4. To adjust the hardware settings, select the **Hardware** tab.
 - Monitor Type
 - Video Card
 5. To adjust settings for multiple monitors, select the **Dual Head** tab and modify the settings.

ACTIVITY 17-5

Configuring X Windows

Before You Begin:
The GUI login screen of srvB is displayed.

Scenario:
Because your manager would like even novice users to be able to use Linux, you should familiarize yourself with configuring X Windows. This will allow novice users to work in a GUI environment, which is more comfortable if they are moving to Linux with some personal computing experience.

What You Do	How You Do It
1. Log in to GNOME and view the display settings.	<div>a. At the login screen, type <i>root</i> and press Enter.</div> <div>b. For the password, type <i>p@ssw0rd</i> and press Enter.</div> <div>c. Choose System→Administration→Display.</div>

2. Adjust the resolution.
 - a. Change the resolution to 640x480.
 - b. To accept the changes, click **OK**.
 - c. In the message box, click **OK**.
 - d. To restart the X server, press **Ctrl+Alt+Backspace**.
 - e. Log in as **root** in the GUI.
 - f. Choose **System→Administration→Display**.
 - g. Verify that the resolution has changed to 640x480.

 3. Verify that the video card and monitor type are set correctly.
 - a. Select the **Hardware** tab.
 - b. Verify that the monitor is set to the monitor you are currently using.
 - c. Verify that the video card is set to the one you are currently using.
 - d. In the **Display Settings** dialog box, click **OK**.
 - e. In the message box, click **OK**.
-
-

Lesson 17 Follow-up

In this lesson, you installed the Linux operating system. You also performed pre-installation and post-installation tasks and documented your actions. These steps ensured your successful installation of the Linux operating system.

1. How does the boot process affect the applications installed on a system? Why?

LESSON 17

2. Which is the best runlevel to boot a system? Why?

LESSON 18

Configuring the GUI

Lesson Time*1 hour(s)*

In this lesson, you will configure the GUI.

You will:

- Implement X.
- Customize the display manager.
- Customize the window environment.
- Configure accessibility settings.

Introduction

In the previous lessons, you used the CLI to perform tasks in Linux. However, for those who are not comfortable with the CLI, Linux also provides a more user-friendly GUI for system management and maintenance tasks. In this lesson, you will configure the GUI.

Linux provides the flexibility of switching back and forth between the CLI and the GUI. While the command line allows you to perform an action with speed, the GUI is more user friendly and allows you to find options and functions easily when you cannot remember the corresponding commands.

This lesson covers all or part of the following CompTIA Linux+ Powered by LPI certification objectives:

- Topic A:
 - Objective 106.1, Objective 106.2
- Topic B:
 - Objective 106.2
- Topic C:
 - Objective 102.4
- Topic D:
 - Objective 106.3

TOPIC A

Implement X

In the last lesson, you performed post-installation tasks. Sometimes, when you are guiding users through a process, they may not understand the commands you tell them to type in the CLI. In such situations, you can choose the GUI because it is more user friendly. Combining the GUI and the CLI in Linux provides users with greater control and a greater number of options. In this topic, you will implement X to work with the GUI.

Because Linux provides both the CLI and GUI, users can choose to work in either one of them or both. Some users may not like the blank screen of the command line. They may prefer to work with more user-friendly icons and windows. Also, they may not always remember the commands to carry out a task. In such cases, they can use the GUI to accomplish the task.

X.Org

X.Org is a free version of the X Window GUI system for some Linux distributions. It provides an interface between input hardware, such as the mouse and the keyboard, and the desktop environment. It is platform independent and extensible because it can be modified by changing or adding new features.

X Servers

Definition:

An *X server* is a program that implements the GUI by providing the X Window system. It runs on a local machine and manages the keyboard, mouse, and display device. It converts the X Windows protocol commands to machine language commands. It also converts the GUI commands to X Windows protocol commands for clients. An X server can draw pictures and display text on screen.

Example:

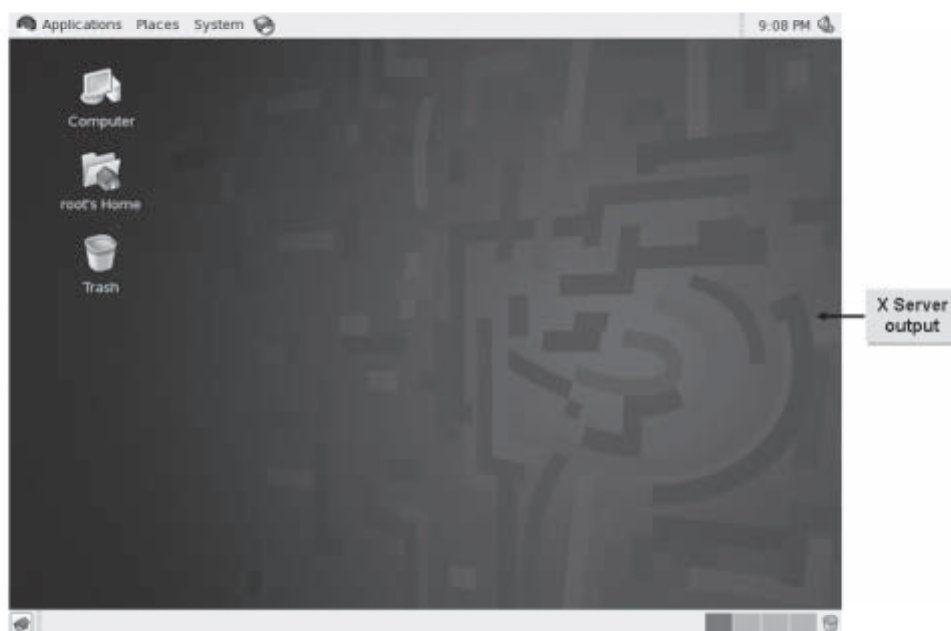


Figure 18-1: The GUI desktop.

The X Protocol

The *X protocol* is the standard protocol used by clients and servers in the X Window system. Using this protocol, requests for window operations can be exchanged.

The xdpypinfo Utility

The `xdpypinfo` utility displays information about the X server. The details displayed include values of parameters related to communication between clients and server, available screen types, and available visual types. By default, the utility displays statistics related to the X server. The statistics cover details such as the name of display, version number, vendor details, and pixmap formats.

The xwininfo Utility

The `xwininfo` utility displays information about the currently selected window in the GUI. The window can be selected by using the mouse, specifying its id, or specifying its name. The details displayed include the window id; the position of the four window coordinates, width, height, color, and depth; and various states of the window such as Bit Gravity State, Window Gravity State, and Map State.

X Clients

Definition:

An *X client* is an application that is written with the aid of the Xlib library, which gives programs access to any X server. An X client sends requests to the X server for a certain action to take place, for example, to create a window. In response to the request, the X server sends the event that the X client is expecting. An X client also receives errors in requests from the server. There can be more than one X client sending requests to the X server.

Example:

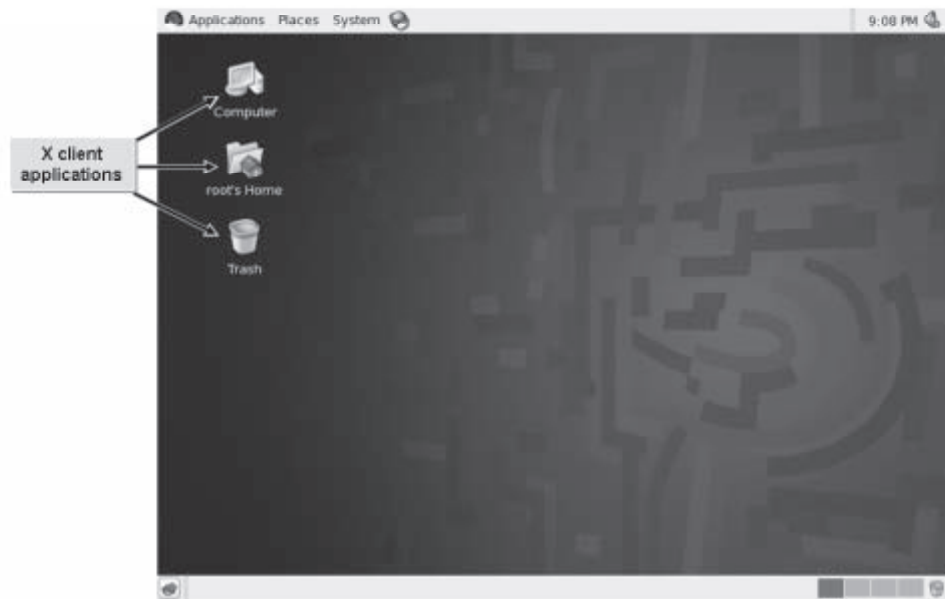


Figure 18-2: X client applications on the desktop.

X Font Servers

Definition:

An *X font server (Xfs)* is a service that provides fonts to the X server and X client applications that connect to the X server. The `/etc/init.d/xfs` script starts the Xfs server. The *font path*, which is a collection of paths in the filesystem where font files are stored, can also be edited using Xfs. Fonts may be stored on one machine, which acts as a networked font server. Multiple X servers can share these fonts over the network. Xfs supports the TrueType, Type1, and bitmap fonts.

Example:

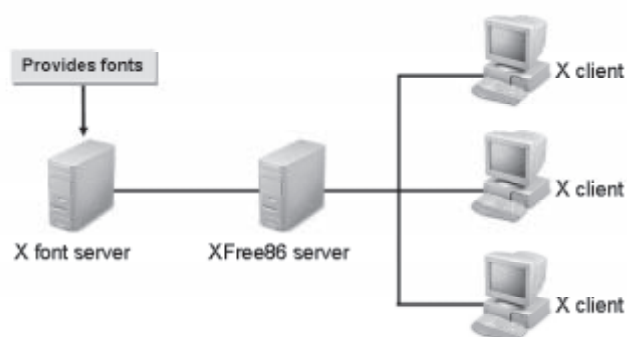


Figure 18-3: The X font server providing fonts to clients.

XOrg Runlevels

The X Window system boots in two main runlevels: runlevel 3 and runlevel 5. When you start a machine, it boots in graphical mode, which is runlevel 5. You can also boot the machine in CLI or text mode, which is runlevel 3. Runlevel 3 is full multiuser mode. The X server is started from runlevel 3 using the `startx` or `xinit` command.

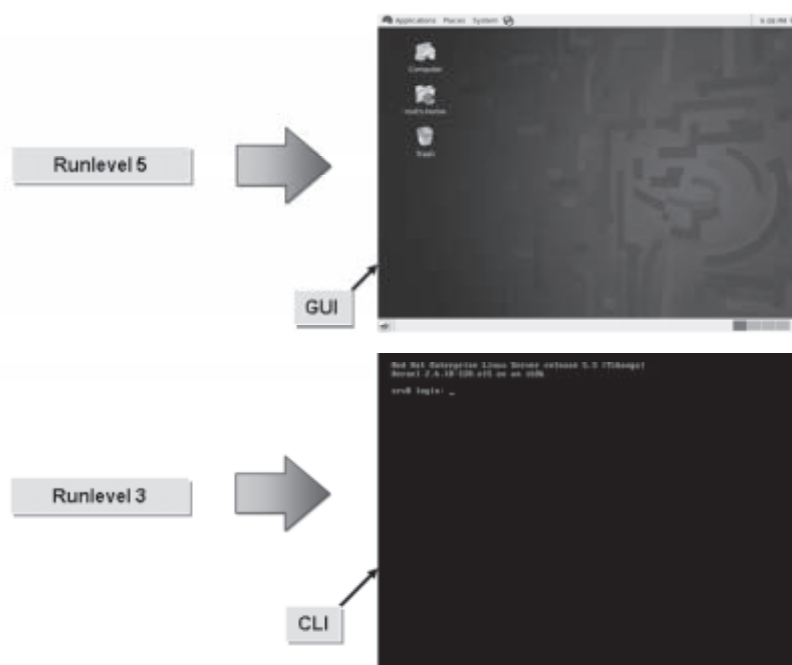


Figure 18-4: Booting in different runlevels results in different displays.

Remote X Sessions

Definition:

Remote X sessions are sessions where a user on a remote workstation is able to view the X Window of the host and run the host's applications. These sessions can run on local and TCP/IP networks. Remote X sessions can be either host based or user based. Host-based sessions are implemented by invoking the `xhost` command, which allows the user to add or remove hosts. User-based sessions are implemented by the `xauth` utility, which authorizes users who can access the remote X host using keys.

Example:

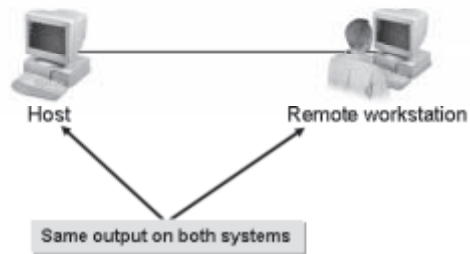


Figure 18-5: Remote X session over a network.

Commands Used in Remote X Sessions

The `xhost` and `xauth` commands are used to manage remote X sessions. A number of options are provided for effective session management.

Option	Enables You To
<code>xhost - help</code>	Display a usage message.
<code>xhost +{name}</code>	Add a name to the list of hosts or users connecting to the X server.
<code>xhost -{name}</code>	Remove a name from the list of hosts or users connecting to the X server.
<code>xauth -f {authfile}</code>	Set the authority file to be used by <code>xauth</code> .
<code>xauth -i</code>	Let <code>xauth</code> bypass authority file locks.
<code>xauth -v</code>	Let <code>xauth</code> print status messages.

X-Stations

Definition:

An *X-station* is a terminal or diskless workstation that is connected to a network and engineered to run the X Window system remotely. An X-system is not directly connected to a computer's CPU. All X-station systems on a network are connected to a central workstation. The central workstation provides the terminals with the operating system, memory, programs, and CPU cycles.

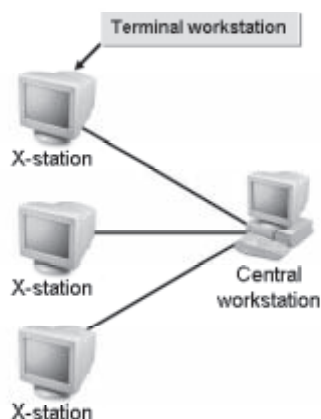
Example:

Figure 18-6: X-station systems connected to a central workstation on a network.

How to Implement X

Procedure Reference: Customize X for the Monitor Automatically

To customize X for the monitor automatically:

1. Log in as root in the GUI.
2. In the warning box that appears, click **Continue**.
3. To display the terminal, choose **Applications→Accessories→Terminal**.
4. To open the Display Settings window, in the terminal, enter `system-config-display`.
5. Select the **Hardware** tab.
6. Customize the monitor settings.
 - a. In the **Monitor Type** section, click **Configure**.
 - b. To expand the **Monitor** section, click the triangle.
 - c. Make necessary changes to the monitor settings.
 - d. To save the settings in the `/etc/X11/xorg.conf` file, select the appropriate monitor model and click **OK**.
7. To close the Display Settings window, click **OK**.
8. At the prompt, click **OK**.
9. To log out of the GUI, choose **System→Log Out root**.
10. Log in for the changes to take effect.



The X Window automatically detects the type of monitor and its settings. If you need to customize the monitor type, refer to the corresponding monitor's product manual to learn its type and optimum settings. Monitor type refers to the different models, sizes, and whether it is a generic or laptop display.

The system-config-display Command

The `system-config-display` command displays the **Display Settings** dialog box to set the system resolution, color depth, and other advanced display settings.

Procedure Reference: Customize X for the Monitor Manually

To customize X for the monitor manually:

1. Log in as root in the CLI.
2. To navigate to the `/etc/X11` folder, enter `cd /etc/X11`.
3. To open the X configuration file, enter `vi xorg.conf`.
4. Below the **Section “Screen”** column, make necessary changes to the monitor settings.
5. Save and close the file.
6. Log out and log in for the changes to take effect.

Procedure Reference: Change Default Bitplanes for the Display Manager

To change the default bitplanes for the display manager:

1. Log in as root in the GUI.
2. To display the terminal, choose **Applications→Accessories→Terminal**.
3. Enter `system-config-display`.
4. From the **Resolution** drop-down list, select the desired resolution.
5. From the **Color Depth** drop-down list, select the desired color depth.
6. To save the settings, click **OK** two times.
7. Choose **System→Log Out root**.
8. In the **Log out of this system now** dialog box, click **Log Out**.
9. Log in again to verify the applied settings.



Bitplanes refer to the display resolution.

Refresh Rate

Refresh rate or vertical scan rate is the speed at which a screen is refreshed. Normally, color displays are refreshed 60 times per second.

Resolution and Color Depth

Resolution is the number of pixels that a computer monitor is capable of displaying. It is described in terms of Width x Height. The most common resolutions are 640 x 480, 800 x 600, and 1024 x 768.

Color depth refers to the number of colors used to display an image. The values can range from 256 colors to millions of colors. The size of a file increases with the increase in the color depth value.

Procedure Reference: Customize X for the Video Card

To customize X for the video card:

1. Log in to the terminal as root.
2. Enter `system-config-display`.
3. Select the **Hardware** tab.
4. Customize X for the video card.
 - a. In the **Video Card** section, click **Configure**.
 - b. Select the appropriate video card and driver settings.
 - c. To save the settings, click **OK** two times.



The X Window automatically detects the type of video card and its driver settings. You can also refer to the product manual to learn the type and optimum settings of the video card.



Every video card comes with a default memory requirement in the form of RAM, which is required for the video card to perform optimally. For normal graphics support, the default memory requirement is 32 MB RAM. If you use graphic-intensive applications, you may need to allocate higher RAM space for optimal performance, provided, your video card supports it. You need to check the product manual of the video card for configuration details.

The xvidtune Command

The `xvidtune` command displays the **xvidtune** dialog box to configure the horizontal and vertical display settings.



This command, when wrongly used, may cause permanent damage to the monitor or video card. Therefore, you must ensure that you do not change any setting without fully understanding the purpose of the setting.

Procedure Reference: Install Fonts

To install fonts:

1. Log in as root in the GUI.
2. To display the terminal, choose **Applications**→**Accessories**→**Terminal**.
3. Create a directory and copy the font into the directory.
 - a. To create the font directory, enter `mkdir /{directory name}`.
 - b. Enter `cp /{directory containing fonts}/{font name}.ttf /{directory name}`.
 - c. Enter `cd /{directory name}`.
4. Create the files `fonts.scale` and `font.dir` in the new directory.
 - a. Enter `ttmkfdir -d /{directory name} -o /{directory name}/fonts.scale`.
 - b. Enter `mkfontdir /{directory name}`.
5. To add the new directory to the default font server configuration file, `/etc/X11/fs/config`, enter `chkfontpath -a /{directory name}`.
6. If necessary, to view the newly added font path, enter `chkfontpath --list`.

7. To restart the xfs service, enter `service xfs restart`.
8. To display the **Font Preferences** dialog box, choose **System**→**Preferences**→**Fonts**.
9. Click the menu button next to **Application font**.
10. In the **Pick a Font** dialog box, in the **Family** list, select the installed font.
11. Click **OK** and click **Close**.

The xorg.conf File

The xorg.conf file is a configuration file for XOrg. This file is used for configuring different X Window parameters and is located in the `/etc/X11/xorg.conf` directory.

Procedure Reference: Configure X to Use the Font Server

To configure X to use the font server:

1. Log in as root in the CLI.
2. To restart the X font server, enter `service xfs restart`.
3. If necessary, to make Xfs available at system startup, enter `chkconfig xfs on`.
4. To start the X Window, enter `startx`.

Procedure Reference: Configure XOrg in Runlevel 3

To configure XOrg in runlevel 3:

1. Log in as root in the CLI.
2. To boot in runlevel 3, enter `init 3`.
3. To start the X server from the command line, enter `xinit`, `startx`, or `init 5`.

Procedure Reference: Configure XOrg in Runlevel 5

To configure XOrg in runlevel 5:

1. Log in as root.
2. To open the `inittab` file, at the command prompt, enter `vi /etc/inittab`.
3. To boot in runlevel 5, ensure that the line `id: runlevel: initdefault` reads `id:5:initdefault`.
4. Save and close the file.
5. Restart the computer.

Procedure Reference: Export X Sessions

To export X sessions:

1. Log in as root in the GUI.
2. To set the display variable, at the terminal, enter `DISPLAY={client IP address}:0.0`.



DISPLAY is an environment variable that is used to specify where to export the X display.

3. Log in as root in the client machine in the GUI.
4. To add the server to the list of hosts, enter `xhost +{server IP address}`.

ACTIVITY 18-1

Configuring X Font Servers

Data Files:

- MalOf.ttf

Before You Begin:

1. You have logged in as root in the GUI of srvA.
2. Display the terminal window.
3. To check if the `libFS-1.0.0-3.1.i386.rpm` package is installed, in the terminal window, enter `rpm -qi libFS`.
4. To check if the `xorg-x11-xfs-1.0.2.4.i386.rpm` package is installed, enter `rpm -qi xorg-x11-xfs`.
5. To check if the `chkfontpath-1.10.1-1.1.i386.rpm` package is installed, enter `rpm -qi chkfontpath`.
6. Copy the `MalOf.ttf` file from `/085099Data/Graphical_User_Interface` to the `/root` directory.
7. To clear the terminal window, enter `clear`.

Scenario:

You are setting up computers for new employees in various divisions of your organization. A new employee in the graphics department requires Linux GUI with high resolution and color settings. The employee also wants the `MalOf.ttf` font installed on the system.

LESSON 18

What You Do	How You Do It
1. Install the new font.	<ol style="list-style-type: none">To create a font directory, enter mkdir /usr/share/fonts/localTo copy the font file to the /usr/share/fonts/local directory, enter cp /root/MalOtf.ttf /usr/share/fonts/localTo navigate to the local directory, enter cd /usr/share/fonts/localEnter ttmkfdir -d /usr/share/fonts/local -o⇒ /usr/share/fonts/local/fonts.scaleEnter mkfontdir /usr/share/fonts/localEnter chkfontpath -a /usr/share/fonts/local
2. Configure the new font.	<ol style="list-style-type: none">To restart the xfs service, enter service xfs restartTo clear the terminal window, enter clearTo display the Font Preferences dialog box, choose System→Preferences→Fonts.Click the menu button next to Application font.In the Pick a Font dialog box, in the Family list, scroll up and select MalOtf and click OK.Click Close.

ACTIVITY 18-2

Configuring XOrg Server

Before You Begin:

- 1. You have logged in as root in the GUI.
- 2. The terminal window is displayed.

Scenario:

Kevin, a user on your network, wants to view the X Window of his system on the environment system, which is on the same network. You are assigned the task of setting up his system. You decide to configure the X server and check if it is in the proper runlevel. You decide to export the X session to the environment system.

What You Do	How You Do It
1. Configure the boot runlevel.	<ul style="list-style-type: none">a. To open the inittab file, enter vi /etc/inittabb. Verify that the line id:{runlevel}:initdefault: reads id:5:initdefault: to boot in runlevel 5.c. Close the file.
2. Export X sessions.	<ul style="list-style-type: none">a. To export the X session, enter DISPLAY=192.168.0.2:0.0b. To close the terminal window, enter exitc. To log out of the system, choose System→Log Out root.d. To log out of the system, in the message box, click Log Out.

TOPIC B

Customize the Display Manager

In the last topic, you implemented X to work with the Linux GUI. Now, you want to customize the GUI environment. In the GUI, the desktop is one of the first screens that a user interacts with. Therefore, it is necessary that the desktop be appealing and easy to use. In this topic, you will customize the display manager to manage the desktop environment.

The desktop is an important part of any GUI. Users may want to customize their desktop environments according to their preferences. They can keep applications that they access frequently and shortcuts to different programs on the desktop. This will enable easy access to various applications and options.

Display Managers

Definition:

A *display manager*, or *window manager*, is a program that controls the look and feel of a desktop environment. The display manager provides a graphical login screen and manages a collection of X servers. These servers may be on the local host or on remote systems. Display managers can be customized to run every time the system boots. The most popular desktop environments that are used by users are GNOME and KDE.

You can customize any of the applications present in the **Applications**, **Places**, or **System** folders for KDE and GNOME. After saving the settings, they will then be applied to the desktop environment. Most of the applications are common to both KDE and GNOME, while some are specific to the individual environment, such as **Control Center** in KDE.

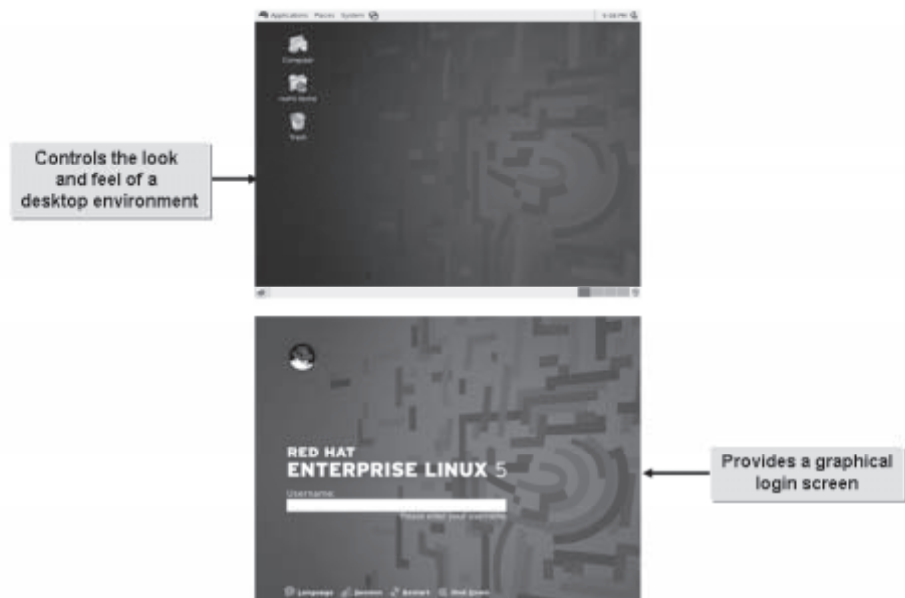
Example:

Figure 18-7: Output of the display manager.

Display Managers for Linux

Common display managers for Linux are as follows:

- The *GNOME Display Manager (GDM)* is the default display manager for Red Hat Linux. GDM allows users to configure language settings, log in, shut down, or reboot the system.
- The *KDE Display Manager (KDM)* is the display manager for KDE, or K Desktop Environment. It allows users to log in, shut down, or reboot the system.
- The X Display Manager, or *xm*, is a basic display manager that allows the user to log in, shut down, or reboot the system.

The GNOME Desktop Environment

The GNOME desktop environment (GDE) is the default desktop environment in most Linux distributions. The GNOME desktop initially displays three icons: **Computer**, **root's Home**, and **Trash**. There are two horizontal panels, one at the top and one at the bottom of the desktop. A user can customize these panels with shortcuts to applications that are frequently used. GDM is used to customize GDE.



Figure 18-8: The GDM with its various components.

The KDE Desktop Environment

The KDE desktop environment is installed along with GDE in some distributions such as RHEL 5. In KDE, there is only one horizontal panel, at the bottom of the desktop. In RHEL 5, the main menu can be accessed by clicking the **Red Hat** logo at the bottom-left corner of the KDE panel. KDE can be customized to suit users' needs.

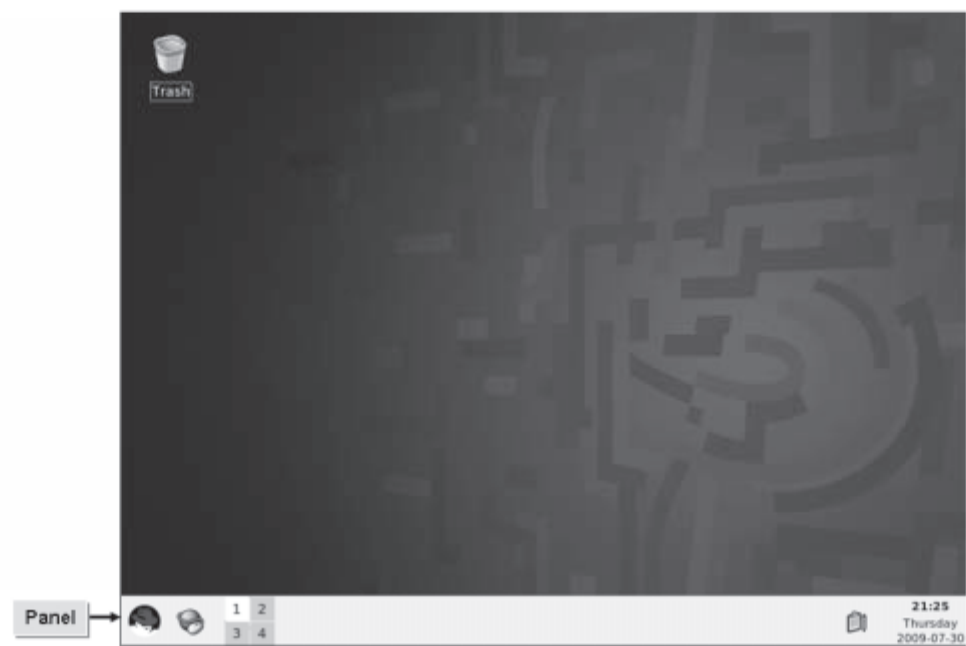


Figure 18-9: The KDE display manager displaying only one panel.

Configure KDM

The Configure - KDesktop window enables you to customize the appearance of KDM. The options that are available in the Configure - KDesktop window are provided in the following table.

Configure - KDesktop Option	Used To
Display	Configure the resolution and other display settings.
Behavior	Configure the behavior of the desktop, such as enabling icons on the desktop and the action to be performed on clicking the right, left, or middle mouse button.
Multiple Desktops	Configure the number of virtual desktops. For example, you can specify up to 20 virtual desktops in RHEL.
Background	Change the background settings such as wall-paper and background.
Screen Saver	Set a screen saver and its timing options.

KDE Panel Configuration Options

The **Add Applet**, **Add Application**, and **Add New Panel** options are used to access and configure different applications that are categorized under **Applet**, **Application Button**, and **Panel**. Some of the options on each menu are provided in the following table.

Add Applet	Add Application	Add New Panel
Clock	The Internet	Panel
Lock/Logout Buttons	Office	Dock Application Bar
Quick Launcher	Find Files/Folders	External Taskbar
Trash	Control Center	KasBar
System Monitor	Help	Universal Sidebar

The switchdesk Command

The `switchdesk` command provides a simple method of switching among various desktop environments. To enable this command, the packages `switchdesk-4.0.8-6.noarch.rpm` and `switchdesk-gui-4.0.8-6.noarch.rpm` have to be installed after the installation of the Linux operating system is complete. On running the `switchdesk` command, the **Desktop Switcher** dialog box is displayed.

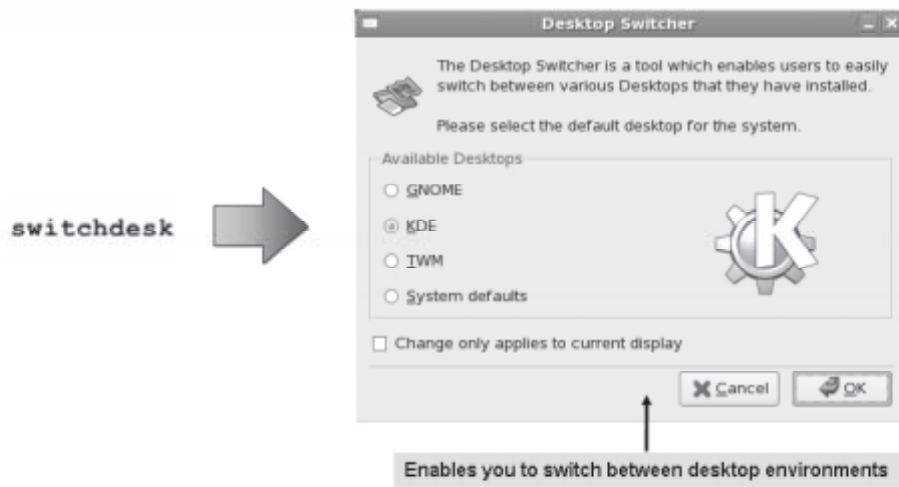


Figure 18-10: The Desktop Switcher dialog box is used to switch between desktops.

How to Customize the Display Manager

Procedure Reference: Switch Between Desktop Environments

To switch between desktop environments:

1. Log in as root in GUI.
2. Display the terminal window.
3. To enable the `switchdesk` feature, verify that the packages `switchdesk-{version}.{release}.rpm` and `switchdesk-gui-{version}.{release}.rpm` are installed.
4. To display the Desktop Switcher window, enter `switchdesk {Desktop type}`.
5. Choose the desired desktop environment.

6. To apply the changes, click **OK** two times.
7. To verify the applied changes, log out and log in.

Procedure Reference: Configure GDM

To configure GDM:

1. Log in as root in the GNOME desktop environment.
2. Choose **Applications→System Tools→Terminal**.
3. To open the **Login Window Preferences** dialog box, enter `gdmsetup`.
4. Make the necessary changes.
5. Click **Close**.

Configure GDM Using the CLI

To configure GDM using the CLI, navigate to the `/etc/X11/gdm/gdm.conf` file. You can manually change the necessary settings, which will then be applied to the desktop after you save and exit the file and start the X Window service.

Procedure Reference: Configure KDM Using the Configure - KDesktop Window

To configure KDM using the Configure - KDesktop window:

1. Log in as root on the KDE desktop.
2. Right-click the desktop and choose **Configure Desktop**.
3. In the Configure - KDesktop window, configure the settings.
 - To modify the background settings, select **Background**.
 - To configure the desktop behavior, select **Behavior**.
 - To configure multiple virtual desktops, select **Multiple Desktops**.
 - To modify the screen saver settings, select **Screen Saver**.
 - To modify the display settings, select **Display**.
4. In the Configure - KDesktop window, click **Apply** and then click **OK**.



To configure KDM using the CLI, navigate and open the `/etc/X11/xdm/kdmrc` file. You can manually change the necessary settings, which will be applied to the desktop after you save and exit the file and start the X window service.

Procedure Reference: Change the XDM Login Screen Logo

To change the logo of XDM login screen:

1. Boot the system in runlevel 3.
2. Log in as root in CLI mode.
3. Enter `cd /etc/X11/xdm`.
4. If necessary, to list all the files in the xdm folder, enter `ls`.
5. Enter `vi Xresources`.



Xresources is a global resources file that is used to customize the login screen.

6. To customize the logo, change `xlogin*logoFileName:`
`/usr/share/xdm/pixmaps/xorg.xpm` to `xlogin*logoFileName:`
`/usr/share/xdm/pixmaps/[Logo name].xpm`.



You can add your own custom logos to the xdm login screen. The logo files must have the .xpm extension and be placed in the `/usr/share/xdm/pixmaps/` directory.

7. Save and close the file.
8. To start the X Display Manager and verify the changes made, enter `xdm`.

Configure XDM

xdm can be configured by means of modifying the relevant files located in the `/etc/X11/xdm/` directory. The files used to configure xdm and their purpose are given in the following table.

If You Need To	Use This File
Configure the graphical login screen.	<code>Xsetup_0</code>
Configure the background image of the XDM.	<code>GiveConsole</code>
Configure user-specified sessions.	<code>Xsession</code>
Configure the startup options of XDM.	<code>xdm-config</code>
Configure X servers running on local machines.	<code>Xserver</code>
Configure remote X servers.	<code>Xaccess</code>

Procedure Reference: Configure Display Managers for Use by X Stations

To configure the desired display managers for use by X stations:

1. Log in as root in the GUI.
2. To display the **Desktop Switcher** dialog box, enter `switchdesk`.
3. Choose the desired desktop environment.
4. To apply the changes, click **OK** two times.
5. To verify that the system boots in the specified desktop, reboot the system.

Procedure Reference: Change the GDM Greeting Page

To change the **GDM greeting** page:

1. Log in as root on the GNOME desktop environment.
2. Choose **Applications**→**Accessories**→**Terminal**.
3. To display the **Login Window Preferences** dialog box, enter `gdmsetup`.
4. In the **Login Window Preferences** dialog box, select the **Local** tab.
5. In the **Themes** section, choose the desired greeting page.
6. Click **Close**.
7. To close the terminal window, enter `exit`.

- 8. Choose **System→Log Out root**.
- 9. In the **Log out of this system now** dialog box, click **Log Out**.

 Instead of using the `switchdesk` command to switch between desktops, you can switch between desktops from the welcome screen. Click the **Session** button at the bottom of the welcome screen and select the appropriate desktop.

ACTIVITY 18-3

Configuring KDM

Before You Begin:

- 1. Switch to `srvB`.
- 2. You have logged in as `root` in the GUI of `srvB`.
- 3. Log out of the `root` user account.

Scenario:

Robin, an employee working in the graphics department, wants to create a customized desktop environment. His requirements include changing the default background, having six desktop windows, and adding the menu bar at the top of the screen. You are assigned the task of changing Robin’s desktop background. You find that Robin presently has GDM configured on his system.

What You Do	How You Do It
1. Switch from GNOME to KDE.	<ul style="list-style-type: none">a. On the welcome screen of the GUI, click Session.b. In the Sessions dialog box, select the KDE option and click Change Session.c. In the Username text box, type <i>root</i> and press Enter.d. In the Password text box, type <i>p@ssw0rd</i> and press Enter.e. To retain the current default session, in the message box that allows you to make the selected session as default, click Just For This Session.

2. Change the desktop background image.
 - a. On the KDM desktop, right-click and choose **Configure Desktop**.
 - b. In the **Configure - KDesktop** dialog box, in the left pane, verify that **Background** is selected.
 - c. In the right pane, in the **Background** section, click the **Picture** drop-down list.
 - d. In the **Picture** drop-down list, scroll up and select **Kubical**.

3. Add the menu bar at the top of the screen.
 - a. In the left pane, select **Behavior**.
 - b. In the **Menu Bar at Top of Screen** section, select the **Desktop menu bar** option.

4. Configure virtual desktops.
 - a. In the left pane, select **Multiple Desktops**.
 - b. In the **Number of desktops** spin box, double-click and type **6**

5. Apply new settings.
 - a. To apply the settings, in the **Configure - KDesktop** dialog box, click **Apply**.
 - b. To close the **Configure - KDesktop** dialog box, click **OK**.

TOPIC C

Customize the Window Environment

In the previous topic, you customized the display manager to manage the desktop environment. In addition to the desktop, windows and icons form an important part of a user's interaction with the GUI. In this topic, you will customize the window environment.

While working in the GUI, users will need to work with windows. They may need to manipulate the size and placement of windows to suit their needs. This makes it essential for users to know how to customize the window environment in Linux.

The Window Environment

Definition:

The window environment is the GUI screen with which users interact. It allows users to control and manipulate the appearance of windows, by modifying their size and placement. It also provides users with icons, taskbars, title bars, and other desktop objects.

Example:

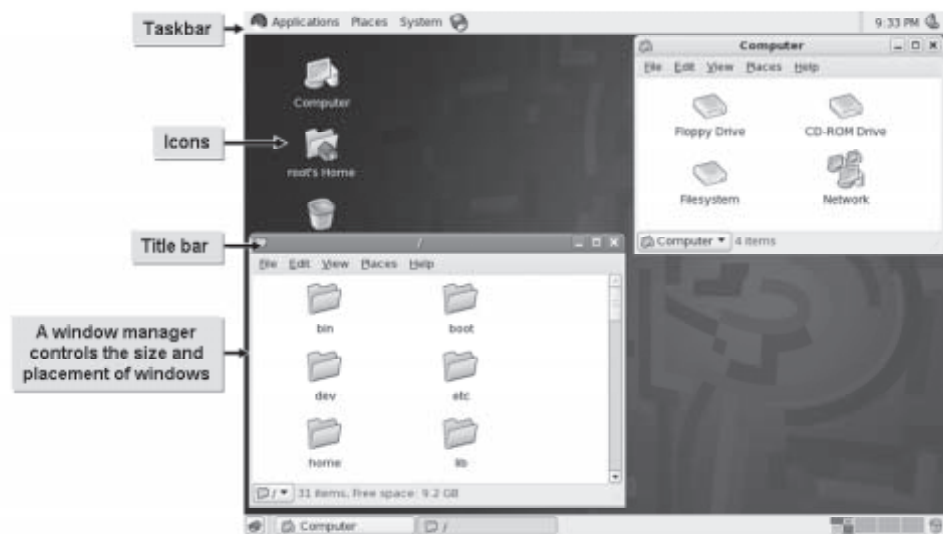


Figure 18-11: Desktop objects of a window environment.

The XTerm

Definition:

The *XTerm* is a screen for typing system commands for the X Window system. It is also known as the shell prompt, console, or terminal. It requires an X server running on the local or remote system. It combines the advantages of the shell and window manager user interfaces.

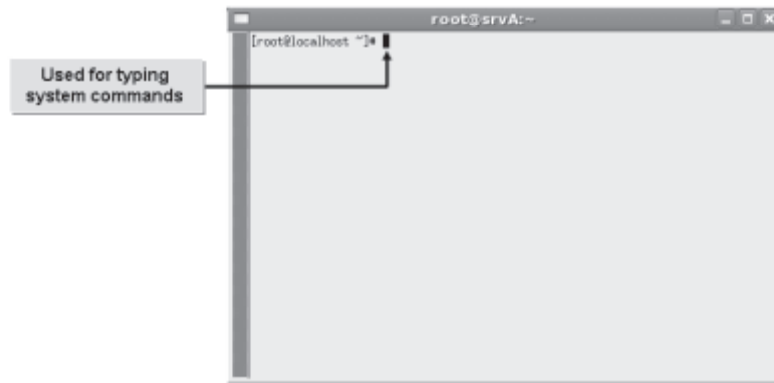
Example:

Figure 18-12: The XTerm window.

How to Customize the Window Environment

Procedure Reference: Customize a System-Wide Desktop Environment

To customize a system-wide desktop environment for KDE or GNOME:

1. Log in as root in the GUI.
2. To access the menu, on the desktop, click the **Start Here** icon in KDE.
3. To access the respective contents and applications in GDE, click the **Applications, Places,** or **System** folder.
4. Make the necessary changes and save the settings.

Procedure Reference: Customize the Window Manager Menu

To customize the window manager menu in GNOME:

1. Customize the window manager menu in GNOME.
 - a. Log in as root in the GNOME GUI.
 - b. To add an application to the panel, right-click the empty space in the panel, which is located at the bottom of the screen, and choose **Add to Panel**.
 - c. Choose the desired application and click **Add**.
 - d. To close the **Add to Panel** dialog box, click **Close**.
 - e. To move an application icon in the panel, right-click the icon, choose **Move** and then move the cursor to the desired location in the panel and click on the panel.
 - f. If necessary, to delete an application icon from the panel, right-click the icon and choose **Remove From Panel**.
2. Position the panels in GNOME.
 - a. Right-click the empty space in the panel, which is located at the bottom of the screen.
 - b. Choose **New Panel** and choose the desired options.
 - c. To change the orientation, size, and color of the panel, right-click the panel and choose **Properties**.

Procedure Reference: Configure a Panel in KDE

To configure a panel in KDE:

1. Log in as root in the KDE GUI.
2. Right-click the empty space in the panel and choose **Configure Panel**.
3. To configure the panel, in the **Configure – KDE Panel** dialog box, use the **Arrangement**, **Appearance**, and **Taskbar** options in the left pane.
 - The **Arrangement** option is used to change the position, length, and size of the panel.
 - The **Appearance** option is used to change the appearance of the panel.
 - The **Taskbar** option is used to configure the actions that need to be performed when clicking the right, left, and middle mouse buttons. It is also used to configure the taskbar.
4. To close the **Configure – KDE Panel** dialog box, click **Apply** to apply the settings and click **OK**.

Procedure Reference: Customize the Window Manager Menu for KDE

To customize the window manager menu for KDE:

1. Log in as root in the KDE GUI.
2. To add an application to the panel, right-click the empty space in the panel, choose **Add Application to Panel** and then choose the desired application. The application icon is added to the panel.
3. To move an application icon in the panel, right-click the icon, click the **Move [Application name]** button, and move the cursor to the desired location in the panel and then click to reposition the panel in the new location.
4. If necessary, to delete an application icon from the panel, right-click the icon and click the **Remove [Application name]** button.



You can add, move, or delete icons used applications in the KDE desktop.

Procedure Reference: Configure xterm

To configure xterm:

1. Log in as root in the GUI.
2. Display the terminal window.
3. Change the location of the xterm window on the screen.
 - a. Enter `vi /etc/X11/xinit/xinitrc`.
 - b. Scroll down and change `xterm -geometry 80x50-50+150`, which sets the location of the xterm window on the screen to `xterm -{parameter} {value}`.
 - c. Save and close the file.



The `etc/X11/xinit` directory contains the `xinitrc` file, which is used to start the window manager.

4. Log out from the current session.
5. To verify that the system boots on the specified desktop, reboot the system.
6. Click **Session**, choose **Failsafe Terminal** and click **OK**.
7. To display the xterm X terminal, enter the user name and password. Ensure that the cursor is within the xterm window.
8. To log out and return to the login screen, enter `exit`.



There are different types of terminals, such as xterm, rxvt, and atterm. The rxvt and atterm are X terminals that are intended as a replacement for xterm. Because they use less swap space than xterm, they are an advantage on any machine serving many X sessions.

Procedure Reference: Verify and Resolve Library Dependency Issues for X Applications

To verify and resolve dependency issues for X applications:

1. To identify the library files and the dependent packages needed for the installation of the X package, enter `rpm -qpR {X application package name}`.
2. To verify that the library files are present in the system, enter `locate {library file}`.
3. To install all the dependencies and then install the required X application packages, enter `rpm -ivh {X application package name}`.

Importance of Library Files

During the installation of certain X applications, the application will search for library files and some dependent packages needed for the X application package to be successfully installed on a system. In case the library files are not installed on the system, you need to first identify the library files and then install the packages containing them along with the dependent packages required for the X application.

ACTIVITY 18-4

Customizing Desktop Panel Menus

Before You Begin:

You have logged in as root in the KDE GUI of srvB.

Scenario:

A new user on your network, Paul, who is just getting familiar with Linux, wants to relocate the edge panel on the desktop to the left and make it compact. Moreover, the user finds it time consuming to access frequently used applications, such as the terminal window and the KWrite application, and also feels that the default panel background color does not suit the panel icons. He asked you to assist and guide him through the task of modifying the desktop.

What You Do	How You Do It
1. Position the panel at the top-left edge of the desktop.	<div>a. In the panel located at the bottom of the screen, right-click the empty space and choose Configure Panel.</div> <div>b. In the Configure - KDE Panel dialog box, verify that Arrangement is selected.</div> <div>c. In the right pane, in the Position section, click the Top left button.</div>
2. Resize the panel.	<div>a. In the Length section, in the Length spin box, double-click and type 50</div> <div>b. In the Size section, from the Size drop-down list, select Small.</div>

3. Change the panel background.
 - a. In the left pane, click **Appearance**.
 - b. In the right pane, in the **Panel Background** section, check the **Enable background image** check box.
 - c. Click the **Open file dialog** icon.
 - d. In the **Select Image File - KDE Panel** dialog box, in the **Location** combo box, double-click and type **/usr/share/wallpapers** and press **Enter**.
 - e. To close the **Select Image File - KDE Panel** dialog box, select **blue_angle_swirl.jpg** and click **OK**.
 - f. To apply the changes and close the **Configure - KDE Panel** dialog box, click **OK**.

 4. Add the frequently used applications to the panel.
 - a. In the panel located at the top-left corner of the screen, right-click the empty space and choose **Add Application to Menubar→System→Terminal**.
 - b. In the panel, right-click the empty space and choose **Add Application to Menubar→Utilities→Editors→KWrite**.
 - c. Choose **K Menu→Log Out**.
 - d. To log out of the KDE session, click **End Current Session**.
-

TOPIC D

Enable Accessibility Settings in Linux

In the previous topic, you customized the window environment. Sometimes, you may be required to modify the computer operating system environment to be usable to users who may have physical or visual disabilities. In this topic, you will enable accessibility settings in Linux.

As a Linux administrator, you need to ensure that all users can use their system with ease. Sometimes, users may have physical or visual disability, which may prevent them from using the default settings available on the system. In such cases, you may need to enable additional keyboard options, sound options, or display themes, so that the users with such disabilities can use their systems with relative ease.

Accessibility Options

Linux provides accessibility options for users to customize Linux and accomplish tasks despite physical and environmental challenges. You need to enable Assistive Technologies (ATs) that support three features, namely Screenreader, Magnifier, and On-Screen Keyboard. Enabling these features before logging on to Linux helps users optimize the Linux environment to suit their needs.

Accessibility Features

The table lists the three accessibility features.

Option	Description
Screen reader	Reads all the highlighted screen elements.
Magnifier	Magnifies the highlighted section on the screen.
On-Screen Keyboard	Enables the on-screen keyboard that you can click to type text using the mouse instead of the regular physical keyboard.

 Orca is a screen reader in Linux.

The GOK - main Window

After you enable the assistive technology option, when you re-login to the system, a new window named GOK-main window will be displayed. GOK stands for GNOME On-Screen Keyboard, a virtual keyboard that can be operated using the mouse. This window contains options that enable users to navigate around the GUI elements with ease.

Keyboard Accessibility Options

Keyboard accessibility options (AccessX) enable additional features that allow users to handle the keys of the keyboard and the mouse in an easier manner.

Keyboard Accessibility Option	Enables Features To
Sticky Keys	Allow users to press one key on the keyboard instead of a combination of several keys at once.
Repeat Keys	Recognize the same keyboard key pressed multiple times by using the time specified for the delay and the number of characters per second specified as the speed.
Slow Keys	Accept only the keystrokes of keys that are held for a specific duration.
Bounce Keys	Avoid unintended successive strokes of a specific key on the keyboard.
Toggle Keys	Enable system beep when toggle keys, such as Num Lock , Caps Lock , or Scroll Lock that illuminate LEDs on the keyboard, are pressed.
Mouse Keys	Allow users to set maximum pointer speed, time to accelerate to maximum speed, and the delay between mouse keypress and pointer movement.

Accessibility Based Themes

Linux contains specific themes that are meant for improving the accessibility of users with visibility problems.

Theme	Displays
High Contrast	The screen using black on white text and black on white icons.
High Contrast Inverse	The screen using white on black text and white on black icons.
High Contrast Large Print	The screen similar to the High Contrast theme with larger text and icons.
High Contrast Large Print Inverse	The screen similar to the High Contrast Inverse theme with larger text and icons.

Orca

Orca is a built-in screen reader in GNOME. Orca allows users to modify settings in the **Orca Preferences** dialog box according to their requirements. Each setting can be enabled by using the check boxes on the tabs of the **Orca Preferences** dialog box.

Tab	Allows You To
Speech	Select either Emacspeak Speech Services or GNOME Speech Services as the Speech system. You can select the desired settings for Speech synthesizer , Voice settings , and Person . In addition, you can set the desired values for Rate , Pitch , and Volume . You can also set the Punctuation Level , Verbosity , and Table Row Speech options. Finally, you can enable speak indentation and justification.
Braille	Enable Braille support, Braille monitor, and Abbreviated role names to enable support for Braille display and specify the desired setting. You can select either Brief or Verbose as the Verbosity option.
Key Echo	Enable key echo for alphanumeric and punctuation keys, modifier keys, locking keys, function keys, and action keys. You can also enable key echo by word.
Magnifier	Select the desired cursor and cross hair settings. You can set the values for Zoomer Settings and Zoomer Position . In addition, you can choose the desired settings for Smoothing and Mouse tracking mode .

How to Configure Accessibility Settings

Procedure Reference: Enable Assistive Technology

To enable assistive technology:

1. Log in as root in the GUI.
2. From the panel, choose **System→Preferences→Accessibility→Assistive Technology Preferences**.
3. To enable assistive technology, in the **Assistive Technology Preferences** dialog box, in the **Support** section, check the **Enable assistive technologies** check box.
4. To enable the assistive technology applications, in the **Applications** section, check the desired check boxes from among the **Screenreader**, **Magnifier**, and **On-screen keyboard** check boxes.
5. To display the **Orca Preferences** dialog box, click **Preferences**.
6. In the dialog box, select the desired tab to enable the settings related to **Speech**, **Braille**, **Key Echo**, and **Magnifier**.
7. To enable assistive technology during login, click **Close and Log Out**.

Procedure Reference: Use Assistive Technology

To use assistive technology:

1. Log in as root in the GUI.
2. If necessary, launch the desired application or terminal.
3. In the GOK - main window, click the desired button.
 - To display the **GOK - Keyboard** dialog box, click **Compose**.
 - To input data to the system, click the desired buttons on the onscreen keyboard.
 - To display the **GOK - move-resize** dialog box, click **Window**.
 - To adjust the size of the dialog box, click the desired buttons.
 - To display the **GOK - mouse** dialog box, click **Mouse**.
 - To select the desired mouse action, click the desired buttons.
 - To display the **GOK - launcher** dialog box, click **Launcher**.
 - To launch **Terminal**, **Web Browser**, **Text Editor**, or **Help Browser**, click the desired buttons.
 - To display the **GOK - Window List** dialog box, click **Activate**.
 - To activate the required window, click the desired buttons.
 - To display the **GOK - gok - controls** dialog box, click **GOK**.
 - To view the **GOK Preferences** dialog box, click **Preferences**. Select the desired tab and modify the setting.
 - To view the **GOK Manual**, click **Help**. Select the desired hyperlink to navigate the contents of the manual.
 - To close the GOK window, click **Quit GOK**. To confirm, in the **GOK - quit** dialog box, click **Really Quit**. If necessary, to display the GOK main window, in the GUI terminal, enter `gok`.
4. If necessary, click **Back** to return to the GOK- main window.
5. To enable the **Menus** button, launch a desired GUI application. To view the **GOK-Menu** dialog box, click **Menus**. To perform a menu action, click the desired menu button.
6. To enable the **Toolbars** button, launch a desired GUI application. To view the **GOK - Toolbars** dialog box, click **Menus**. To select a toolbar, in the dialog box, click the desired toolbar button.
7. To display the **GOK - GUI** dialog box, click **UI Grab**. Navigate around the GUI controls.

Procedure Reference: Enable Keyboard Accessibility Features

To enable keyboard accessibility features:

1. Log in as root in the GUI.
2. From the panel, choose **System**→**Preferences**→**Accessibility**→**Keyboard**.
3. To enable the keyboard accessibility feature, in the **Keyboard Accessibility Preferences (Access X)** dialog box, check the **Enable keyboard accessibility features** check box.

4. On the **Basic** tab, if necessary, check the **Enable Sticky Keys** and **Enable Repeat Keys** check boxes.
5. Select the **Filters** tab. On the **Filters** tab, if necessary, check the **Enable Slow Keys**, **Enable Bounce Keys**, and **Enable Toggle Keys** check boxes.
6. Select the **Mouse Keys** tab. On the **Mouse Keys** tab, check the **Enable Mouse Keys** check box. If necessary, click **Mouse Preferences** and specify the desired setting.
7. To save and close the dialog box, click **Close**.

Procedure Reference: Enable Accessibility Themes

To enable accessibility themes:

1. Log in as root in the GUI.
2. To display the **Theme Preferences** dialog box, from the panel, choose **System→Preferences→Accessibility→Themes**.
3. To enable the accessibility themes, in the list, select either **High Contrast** or **High Contrast Inverse** to preview the theme.
4. If necessary, to display the **Theme Details** dialog box, click **Theme Details**. On the **Controls** tab, select either **High Contrast**, **High Contrast Inverse**, **High Contrast Large Print**, or **High Contrast Large Print Inverse**. Click **Close**.
5. To close the dialog box, click **Close**.

Procedure Reference: Enable Accessibility at GDM Login

To enable accessibility at GDM login.

1. Log in as root on the GNOME desktop environment.
2. Choose **Applications→Accessories→Terminal**.
3. To display the **Login Window Preferences** dialog box, enter `gdmsetup`.
4. In the **Login Window Preferences** dialog box, select the **Accessibility** tab.
5. Check the **Enable accessible login** check box.
6. Click **Close**.
7. To close the terminal window, enter `exit`.
8. Choose **System→Log Out root**.
9. In the **Log out of this system now** dialog box, click **Log Out**.

Gestures at gdm Login

After enabling accessibility at login, you can use gestures, such as sticky keys and mouse actions, to log in to the system.

ACTIVITY 18-5

Enabling Accessibility Settings

Before You Begin:

Log in as root in the GUI.

Scenario:

Your colleague, Peter, fractured his right arm in an accident. Because he is working on a critical project, he has agreed to work from home to complete the project. As a system administrator, you are assigned the task of preparing a Linux laptop so that Peter can complete the project as scheduled without much inconvenience.

What You Do	How You Do It
1. Enable assistive technology.	<div>a. To display the Assistive Technology Preferences dialog box, from the panel, choose System→Preferences→Accessibility→Assistive Technology Preferences.</div> <div>b. In the Support section, check the Enable assistive technologies check box.</div> <div>c. In the Applications section, check the On-screen keyboard check box.</div> <div>d. Click Close and Log Out.</div> <div>e. In the message box, check the Save current setup check box.</div> <div>f. In the Action section, verify that the Log out option is selected and click OK.</div>

LESSON 18

2. Use assistive technology to enable the GNOME On-screen keyboard.
 - a. Log in as root.
 - b. In the **Assistive Technology Preferences** dialog box, click **Close**.
 - c. In the message box, click **OK**.
 - d. To display the **GOK - Keyboard** dialog box, in the GOK- main window, click **Compose**.
 - e. To launch the gedit application, choose **Applications→Accessories→Text Editor**.
 - f. In the **GOK - Keyboard** dialog box, click **q**.
 - g. Observe that the letter q is automatically displayed in the gedit window. In the **GOK - Keyboard** dialog box, click **quality**.
 - h. Observe that the letter "q" is automatically replaced with the word "quality" in the gedit window.
 - i. To return to the GOK-main window, click **Back**. Close the gedit window.
 - j. To close the application without saving the document, in the message box, click **Close without Saving**.
-

Lesson 18 Follow-up

In this lesson, you configured the GUI. Working with the GUI of Linux can be useful when recalling commands becomes difficult. The GUI is user friendly and easy to understand. As a Linux administrator, it will help you direct users to configure their systems.

1. Do you think using the Linux GUI in conjunction with the CLI will yield better results? Why?
2. In what way do you think customizing window managers is useful?

Follow-up

In this course, you acquired the essential skills and information you will need to install, configure, troubleshoot, and perform preventative maintenance of the Linux operating system. If you are getting ready for a career as an entry-level Linux administrator or a computer support technician, and if your job duties require you to work with Linux servers and workstations on day-to-day basis, this course presented you with the background knowledge and skills you will require to be successful. Taking this course was also an important part of your preparation for the CompTIA® Linux+™ Powered by LPI exams (Exam Codes: LX0-101 and LX0-102), in order to become a CompTIA® Linux+™ Certified Professional.

1. Which system feature should be managed properly to maintain the integrity of the system?
2. What are the probable issues that might arise while working with Linux systems?
3. Why is securing Linux systems important? Have you faced any problems with security in your workplace? If yes, how did you tackle them?

What's Next?

The material in *CompTIA® Linux+™ Certification Powered by LPI* provides foundational information and skills required to pursue a career as a Linux administrator or support technician. It also assists you in preparing for the CompTIA® Linux+™ Powered by LPI exams (Exam Codes: LX0-101 and LX0-102), in order to become a CompTIA® Linux+™ Certified Professional. Once you have completed *CompTIA® Linux+™ Certification*, you may wish to continue your certification path by taking any one of the other Element K CompTIA certification courses, *CompTIA® Network+® (2009 Objectives)*, *CompTIA® Security+® (2008 Objectives)*, or *CompTIA® A+® Certification (2009 Objectives)*, each of which prepares you for the associated CompTIA certification exam.

FOLLOW-UP

APPENDIX A

Mapping Course Content to the CompTIA Linux+ Powered by LPI Certification Exam Objectives

The following tables will assist you in mapping the Linux+ Powered by LPI Certification course content to the CompTIA Linux+ Powered by LPI certification exam objectives (Exam Codes: LX0-101 and LX0-102).

101 System Architecture

Exam Objective (LX0-101)	Linux+ Powered by LPI Certification Lesson and Topic Reference
101.1 Determine and Configure hardware settings	
• Enable and disable integrated peripherals	Lesson 17 Topic A
• Configure systems with or without external peripherals such as keyboards	Lesson 15 Topic B
• Differentiate between the various types of mass storage devices	Lesson 3 Topic D Lesson 15 Topic A
• Set the correct hardware ID for different devices, especially the boot device	Lesson 17 Topic C
• Know the differences between coldplug and hotplug devices	Lesson 8 Topic D
• Determine hardware resources for devices	Lesson 8 Topic E Lesson 15 Topic A
• Tools and utilities to list various hardware information (e.g. lsusb, lspci, etc.)	Lesson 8 Topic E

Exam Objective (LX0–101)	Linux+ Powered by LPI Certification Lesson and Topic Reference
101.1 Determine and Configure hardware settings	
• Tools and utilities to manipulate USB devices	Lesson 8 Topic E Lesson 15 Topic B
• Conceptual understanding of sysfs, udev, hald, dbus	Lesson 8 Topic D Lesson 8 Topic E
The following is a partial list of the used files, terms, and utilities:	
• /sys	Lesson 8 Topic D
• /proc	Lesson 8 Topic B
• /dev	Lesson 3 Topic B
• modprobe	Lesson 8 Topic B
• lsmod	Lesson 8 Topic B
• lspci	Lesson 8 Topic E
• lsusb	Lesson 8 Topic E

Exam Objective (LX0–101)	Linux+ Powered by LPI Certification Lesson and Topic Reference
101.2 Boot the System	
• Provide common commands to the boot loader and options to the kernel at boot time	Lesson 8 Topic B Lesson 17 Topic B
• Demonstrate knowledge of the boot sequence from BIOS to boot completion	Lesson 17 Topic B
• Check boot events in the log file	Lesson 16 Topic A
The following is a partial list of the used files, terms and utilities:	
• /var/log/messages	Lesson 11 Topic B
• dmesg	Lesson 16 Topic B
• BIOS	Lesson 17 Topic A Lesson 17 Topic B
• bootloader	Lesson 17 Topic B
• kernel	Lesson 8 Topic A
• init	Lesson 1 Topic D

Exam Objective (LX0–101)	Linux+ Powered by LPI Certification Lesson and Topic Reference
101.3 Change runlevels and shutdown or reboot system	
• Set the default runlevel	Lesson 1 Topic D
• Change between runlevels including single user mode	Lesson 1 Topic D
• Shutdown and reboot from the command line	Lesson 1 Topic D
• Alert users before switching runlevels or other major system events	Lesson 1 Topic D
• Properly terminate processes	Lesson 10 Topic B
The following is a partial list of the used files, terms and utilities:	
• /etc/inittab	Lesson 1 Topic D Lesson 11 Topic A
• shutdown	Lesson 1 Topic D
• init	Lesson 1 Topic D
• /etc/init.d	Lesson 11 Topic A
• telinit	Lesson 1 Topic D

102 Linux Installation and Package Management

Exam Objective (LX0–101)	Linux+ Powered by LPI Certification Lesson and Topic Reference
102.1 Design hard disk layout	
• Allocate filesystems and swap space to separate partitions or disks	Lesson 3 Topic A Lesson 3 Topic C
• Tailor the design to the intended use of the system	Lesson 3 Topic C
• Ensure the /boot partition conforms to the hardware architecture requirements for booting	Lesson 3 Topic A Lesson 3 Topic B Lesson 16 Topic A Lesson 17 Topic C
The following is a partial list of the used files, terms and utilities:	
• / (root) filesystem	Lesson 3 Topic B
• /var filesystem	Lesson 3 Topic B
• /home filesystem	Lesson 3 Topic B
• swap space	Lesson 3 Topic C
• mount points	Lesson 3 Topic C
• partitions	Lesson 3 Topic A

Exam Objective (LX0–101)	Linux+ Powered by LPI Certification Lesson and Topic Reference
102.2 Install a boot manager	
• Providing alternative boot locations and backup boot options	Lesson 17 Topic C
• Install and configure a boot loader such as GRUB	Lesson 17 Topic C
• Interact with the boot loader	Lesson 17 Topic C
The following is a partial list of the used files, terms, and utilities	
• /boot/grub/menu.lst	Lesson 17 Topic C
• grub-install	Lesson 17 Topic C
• MBR	Lesson 17 Topic B
• superbblock	Lesson 17 Topic B

Exam Objective (LX0–101)	Linux+ Powered by LPI Certification Lesson and Topic Reference
102.3 Manage shared libraries	
• Identify shared libraries	Lesson 7 Topic H
• Identify the typical locations of system libraries	Lesson 3 Topic B Lesson 7 Topic H
• Load shared libraries	Lesson 7 Topic H
The following is a partial list of the used files, terms and utilities	
• ldd	Lesson 7 Topic H
• ldconfig	Lesson 7 Topic H
• /etc/ld.so.conf	Lesson 7 Topic H
• LD_LIBRARY_PATH	Lesson 7 Topic H

Exam Objective (LX0–101)	Linux+ Powered by LPI Certification Lesson and Topic Reference
102.4 Use Debian package management	
• Install, upgrade and uninstall Debian binary packages	Lesson 7 Topic F
• Find packages containing specific files or libraries which may or may not be installed	Lesson 7 Topic F

Exam Objective (LX0–101)	Linux+ Powered by LPI Certification Lesson and Topic Reference
102.4 Use Debian package management	
<ul style="list-style-type: none"> Obtain package information like version, content, dependencies, package integrity and installation status (whether or not the package is installed) 	Lesson 7 Topic F Lesson 18 Topic C
The following is a partial list of the used files, terms and utilities:	
<ul style="list-style-type: none"> /etc/apt/sources.list 	Lesson 7 Topic F
<ul style="list-style-type: none"> dpkg 	Lesson 7 Topic F
<ul style="list-style-type: none"> dpkg-reconfigure 	Lesson 7 Topic F
<ul style="list-style-type: none"> apt-get 	Lesson 7 Topic F
<ul style="list-style-type: none"> apt-cache 	Lesson 7 Topic F
<ul style="list-style-type: none"> aptitude 	Lesson 7 Topic F

Exam Objective (LX0–101)	Linux+ Powered by LPI Certification Lesson and Topic Reference
102.5 Use RPM and YUM package management	
<ul style="list-style-type: none"> Install, re-install, upgrade and remove packages using RPM and YUM 	Lesson 7 Topic A Lesson 7 Topic E
<ul style="list-style-type: none"> Obtain information on RPM packages such as version, status, dependencies, integrity and signatures 	Lesson 7 Topic A
<ul style="list-style-type: none"> Determine what files a package provides, as well as find which package a specific file comes from 	Lesson 7 Topic A
The following is a partial list of the used files, terms and utilities:	
<ul style="list-style-type: none"> rpm 	Lesson 7 Topic A
<ul style="list-style-type: none"> rpm2cpio 	Lesson 7 Topic A
<ul style="list-style-type: none"> /etc/yum.conf 	Lesson 7 Topic D
<ul style="list-style-type: none"> /etc/yum.repos.d/ 	Lesson 7 Topic D
<ul style="list-style-type: none"> yum 	Lesson 7 Topic E
<ul style="list-style-type: none"> yumdownloader 	Lesson 7 Topic E

103 GNU and Unix Commands

Exam Objective (LX0–101)	Linux+ Powered by LPI Certification Lesson and Topic Reference
103.1 Work on the command line	
<ul style="list-style-type: none"> Use single shell commands and one line command sequences to perform basic tasks on the command line 	Lesson 1 Topic B
<ul style="list-style-type: none"> Use and modify the shell environment including defining, referencing and exporting environment variables 	Lesson 9 Topic C
<ul style="list-style-type: none"> Use and edit command history 	Lesson 1 Topic B Lesson 9 Topic A Lesson 9 Topic C
<ul style="list-style-type: none"> Invoke commands inside and outside the defined path 	Lesson 1 Topic B
The following is a partial list of the used files, terms and utilities:	
<ul style="list-style-type: none"> . 	Lesson 3 Topic B
<ul style="list-style-type: none"> bash 	Lesson 1 Topic B
<ul style="list-style-type: none"> echo 	Lesson 1 Topic B
<ul style="list-style-type: none"> env 	Lesson 2 Topic B
<ul style="list-style-type: none"> exec 	Lesson 1 Topic B
<ul style="list-style-type: none"> export 	Lesson 9 Topic C
<ul style="list-style-type: none"> pwd 	Lesson 3 Topic B
<ul style="list-style-type: none"> set 	Lesson 2 Topic B
<ul style="list-style-type: none"> unset 	Lesson 2 Topic B
<ul style="list-style-type: none"> man 	Lesson 1 Topic C
<ul style="list-style-type: none"> uname 	Lesson 8 Topic A Lesson 8 Topic F
<ul style="list-style-type: none"> history 	Lesson 9 Topic A

Exam Objective (LX0–101)	Linux+ Powered by LPI Certification Lesson and Topic Reference
103.2 Process text streams using filters	
<ul style="list-style-type: none"> Send text files and output streams through text utility filters to modify the output using standard UNIX commands found in the GNU textutils package 	Lesson 4 Topic D
The following is a partial list of the used files, terms and utilities:	

Exam Objective (LX0–101)	Linux+ Powered by LPI Certification Lesson and Topic Reference
103.2 Process text streams using filters	
• cat	Lesson 4 Topic D
• cut	Lesson 4 Topic D
— expand	Lesson 4 Topic D
— fmt	Lesson 4 Topic D
— head	Lesson 4 Topic D
— od	Lesson 4 Topic D
— join	Lesson 4 Topic D
— nl	Lesson 4 Topic D
— paste	Lesson 4 Topic D
— pr	Lesson 4 Topic D
— sed	Lesson 11 Topic B
— sort	Lesson 4 Topic D
• split	Lesson 4 Topic D
• tail	Lesson 4 Topic D
• tr	Lesson 4 Topic D
• unexpand	Lesson 4 Topic D
• uniq	Lesson 4 Topic D
• wc	Lesson 4 Topic D

Exam Objective (LX0–101)	Linux+ Powered by LPI Certification Lesson and Topic Reference
103.3 Perform basic file management	
• Copy, move and remove files and directories individually	Lesson 3 Topic B
• Copy multiple files and directories recursively	Lesson 3 Topic B
• Remove files and directories recursively	Lesson 3 Topic B
• Use simple and advanced wildcard specifications in commands	Lesson 9 Topic A
• Using find to locate and act on files based on type, size, or time	Lesson 4 Topic B Lesson 9 Topic A
• Usage of tar, cpio, and dd	Lesson 4 Topic F
The following is a partial list of the used files, terms and utilities:	
• cp	Lesson 3 Topic B

Exam Objective (LX0–101)	Linux+ Powered by LPI Certification Lesson and Topic Reference
103.3 Perform basic file management	
• find	Lesson 4 Topic B
• mkdir	Lesson 3 Topic B
• mv	Lesson 3 Topic B
• ls	Lesson 3 Topic B
• rm	Lesson 3 Topic B
• rmdir	Lesson 3 Topic B
• touch	Lesson 3 Topic B
• tar	Lesson 4 Topic F
• cpio	Lesson 4 Topic F
• dd	Lesson 4 Topic F
• file	Lesson 3 Topic B
• gzip	Lesson 4 Topic F
• gunzip	Lesson 4 Topic F
• bzip2	Lesson 4 Topic F
• file globbing	Lesson 9 Topic A

Exam Objective (LX0–101)	Linux+ Powered by LPI Certification Lesson and Topic Reference
103.4 Use streams, pipes and redirects	
• Redirecting standard input, standard output and standard error	Lesson 9 Topic D
• Pipe the output of one command to the input of another command	Lesson 9 Topic D
• Use the output of one command as arguments to another command	Lesson 9 Topic D
• Send output to both stdout and a file	Lesson 9 Topic D
The following is a partial list of the used files, terms and utilities:	
• tee	Lesson 9 Topic D
• xargs	Lesson 9 Topic D

Exam Objective (LX0–101)	Linux+ Powered by LPI Certification Lesson and Topic Reference
103.5 Create, monitor and kill processes	
• Run jobs in the foreground and background	Lesson 10 Topic A
• Signal a program to continue running after logout	Lesson 10 Topic C
• Monitor active processes	Lesson 10 Topic B
• Select and sort processes for display	Lesson 10 Topic B
• Send signals to processes	Lesson 10 Topic B
The following is a partial list of the used files, terms and utilities:	
• &	Lesson 10 Topic A
• bg	Lesson 10 Topic A
• fg	Lesson 10 Topic A
• jobs	Lesson 10 Topic A
• kill	Lesson 10 Topic B
• nohup	Lesson 10 Topic C
• ps	Lesson 10 Topic B
• top	Lesson 10 Topic B
• free	Lesson 8 Topic F
• uptime	Lesson 1 Topic B
• killall	Lesson 10 Topic B

Exam Objective (LX0–101)	Linux+ Powered by LPI Certification Lesson and Topic Reference
103.6 Modify process execution priorities	
• Know the default priority of a job that is created	Lesson 10 Topic B
• Run a program with higher or lower priority than the default	Lesson 10 Topic B
• Change the priority of a running process	Lesson 10 Topic B
The following is a partial list of the used files, terms and utilities:	
• nice	Lesson 10 Topic B
• ps	Lesson 10 Topic B
• renice	Lesson 10 Topic B
• top	Lesson 10 Topic B

Exam Objective (LX0–101)	Linux+ Powered by LPI Certification Lesson and Topic Reference
103.7 Search text files using regular expressions	
• Create simple regular expressions containing several notational elements	Lesson 4 Topic C
• Use regular expression tools to perform searches through a filesystem or file content	Lesson 4 Topic C
The following is a partial list of the used files, terms and utilities:	
• grep	Lesson 4 Topic B Lesson 4 Topic D Lesson 11 Topic B
• egrep	Lesson 11 Topic B
• fgrep	Lesson 11 Topic B
• sed	Lesson 11 Topic B
• regex(7)	Lesson 4 Topic C Lesson 11 Topic B

Exam Objective (LX0–101)	Linux+ Powered by LPI Certification Lesson and Topic Reference
103.8 Perform basic file editing operations using vi	
• Navigate a document using vi	Lesson 4 Topic A
• Use basic vi modes	Lesson 4 Topic A
• Insert, edit, delete, copy and find text	Lesson 4 Topic A
The following is a partial list of the used files, terms and utilities:	
• vi	Lesson 4 Topic A
• /, ?	Lesson 4 Topic A
• h,j,k,l	Lesson 4 Topic A
• i, o, a	Lesson 4 Topic A
• c, d, p, y, dd, yy	Lesson 4 Topic A
• ZZ, :w!, :q!, :e!	Lesson 4 Topic A

104 Devices, Linux Filesystems, Filesystem Hierarchy Standard

Exam Objective (LX0–101)	Linux+ Powered by LPI Certification Lesson and Topic Reference
104.1 Create partitions and filesystems	
Use various mkfs commands to set up partitions and create various filesystems such as:	Lesson 3 Topic A
• ext2	
• ext3	Lesson 3 Topic A
• xfs	Lesson 3 Topic A
• reiserfs v3	Lesson 3 Topic A
• vfat	Lesson 3 Topic A
The following is a partial list of the used files, terms and utilities:	
• fdisk	Lesson 3 Topic A
• mkfs	Lesson 3 Topic A
• mkswap	Lesson 3 Topic C

Exam Objective (LX0–101)	Linux+ Powered by LPI Certification Lesson and Topic Reference
104.2 Maintain the integrity of filesystems	
• Verify the integrity of filesystems	Lesson 3 Topic D Lesson 15 Topic A
• Monitor free space and inodes	Lesson 15 Topic A Lesson 15 Topic C
• Repair simple filesystem problems	Lesson 3 Topic D
The following is a partial list of the used files, terms and utilities:	
• du	Lesson 15 Topic A
• df	Lesson 15 Topic A
• fsck	Lesson 3 Topic D
• e2fsck	Lesson 3 Topic D
• mke2fs	Lesson 3 Topic A
• debugfs	Lesson 3 Topic D
• dumpe2fs	Lesson 3 Topic D
• tune2fs	Lesson 3 Topic D
• xfs tools (such as xfs_metadump and xfs_info)	Lesson 3 Topic D

Exam Objective (LX0–101)	Linux+ Powered by LPI Certification Lesson and Topic Reference
104.3 Control mounting and unmounting of filesystems	
• Manually mount and unmount filesystems	Lesson 3 Topic C
• Configure filesystem mounting on bootup	Lesson 3 Topic A
• Configure user mountable removeable filesystems	Lesson 3 Topic C
The following is a partial list of the used files, terms and utilities:	
• /etc/fstab	Lesson 3 Topic A
• /media	Lesson 3 Topic B
— mount	Lesson 3 Topic C
— umount	Lesson 3 Topic C

Exam Objective (LX0–101)	Linux+ Powered by LPI Certification Lesson and Topic Reference
104.4 Manage disk quotas	
• Set up a disk quota for a filesystem	Lesson 15 Topic C
• Edit, check and generate user quota reports	Lesson 15 Topic C
The following is a partial list of the used files, terms and utilities:	
• quota	Lesson 15 Topic C
• edquota	Lesson 15 Topic C
• repquota	Lesson 15 Topic C
• quotaon	Lesson 15 Topic C

Exam Objective (LX0–101)	Linux+ Powered by LPI Certification Lesson and Topic Reference
104.5 Manage file permissions and ownership	
• Manage access permissions on regular and special files as well as directories	Lesson 5 Topic A
• Use access modes such as suid, sgid and the sticky bit to maintain security	Lesson 5 Topic D
• Know how to change the file creation mask	Lesson 5 Topic B
• Use the group field to grant file access to group members	Lesson 5 Topic C
The following is a partial list of the used files, terms and utilities:	
• chmod	Lesson 5 Topic A

Exam Objective (LX0–101)	Linux+ Powered by LPI Certification Lesson and Topic Reference
104.5 Manage file permissions and ownership	
• umask	Lesson 5 Topic B
• chown	Lesson 5 Topic C
• chgrp	Lesson 5 Topic C

Exam Objective (LX0–101)	Linux+ Powered by LPI Certification Lesson and Topic Reference
104.6 Create and change hard and symbolic links	
• Create links	Lesson 4 Topic E
• Identify hard and/or softlinks	Lesson 4 Topic E
• Copying versus linking files	Lesson 4 Topic E
• Use links to support system administration tasks	Lesson 4 Topic E
The following is a partial list of the used files, terms and utilities:	
• ln	Lesson 4 Topic E

Exam Objective (LX0–101)	Linux+ Powered by LPI Certification Lesson and Topic Reference
104.7 Find system files and place files in the correct location	
• Understand the correct locations of files under the FHS	Lesson 3 Topic B
• Find files and commands on a Linux system	Lesson 4 Topic B
• Know the location and propose of important file and directories as defined in the FHS	Lesson 3 Topic B
The following is a partial list of the used files, terms and utilities:	
• find	Lesson 4 Topic B
• locate	Lesson 4 Topic B
• updatedb	Lesson 4 Topic B
• whereis	Lesson 4 Topic B
• which	Lesson 1 Topic B
• type	Lesson 3 Topic A
• /etc/updatedb.conf	Lesson 4 Topic B

105 Shells, Scripting and Data Management

Exam Objective (LX0–102)	Linux+ Powered by LPI Certification Lesson and Topic Reference
105.1 Customize and use the shell environment	
• Set environment variables (e.g. PATH) at login or when spawning a new shell	Lesson 9 Topic C
• Write BASH functions for frequently used sequences of commands	Lesson 9 Topic E
• Maintain skeleton directories for new user accounts	Lesson 2 Topic B
• Set command search path with the proper directory	Lesson 2 Topic B Lesson 9 Topic C
The following is a partial list of the used files, terms, and utilities:	
• /etc/profile	Lesson 2 Topic B Lesson 7 Topic H Lesson 10 Topic E
• env	Lesson 2 Topic B
• export	Lesson 2 Topic B
• set	Lesson 2 Topic B
• unset	Lesson 2 Topic B
• ~/.bash_profile	Lesson 2 Topic B Lesson 9 Topic D
• ~/.bash_login	Lesson 9 Topic D Lesson 17 Topic B
— ~/.profile	Lesson 9 Topic D
— ~/.bashrc	Lesson 2 Topic B Lesson 9 Topic C Lesson 9 Topic D Lesson 14 Topic B
— ~/.bash_logout	Lesson 9 Topic D
• function	Lesson 9 Topic E
— alias	Lesson 9 Topic C
• lists	Lesson 9 Topic D

Exam Objective (LX0–102)	Linux+ Powered by LPI Certification Lesson and Topic Reference
105.2 Customize or write simple scripts	
• Use standard sh syntax (loops, tests)	Lesson 1 Topic B Lesson 9 Topic B

Exam Objective (LX0–102)	Linux+ Powered by LPI Certification Lesson and Topic Reference
105.2 Customize or write simple scripts	
• Use command substitution	Lesson 9 Topic D
• Test return values for success or failure or other information provided by a command	Lesson 9 Topic B
• Perform conditional mailing to the superuser	Lesson 9 Topic E
• Correctly select the script interpreter through the shebang (!) line	Lesson 9 Topic B
• Manage the location, ownership, execution and suid-rights of scripts	Lesson 9 Topic C
The following is a partial list of the used files, terms, and utilities:	
• for	Lesson 9 Topic E
• while	Lesson 9 Topic E
• test	Lesson 9 Topic B
• if	Lesson 9 Topic E
• read	Lesson 9 Topic D
• seq	Lesson 9 Topic D

Exam Objective (LX0–102)	Linux+ Powered by LPI Certification Lesson and Topic Reference
105.3 SQL data management	
• Use of basic SQL commands	Lesson 4 Topic G
• Perform basic data manipulation	Lesson 4 Topic G
The following is a partial list of the used files, terms, and utilities:	
• insert	Lesson 4 Topic G
• update	Lesson 4 Topic G
• select	Lesson 4 Topic G
• delete	Lesson 4 Topic G
• from	Lesson 4 Topic G
• where	Lesson 4 Topic G
• group by	Lesson 4 Topic G
• order by	Lesson 4 Topic G
• join	Lesson 4 Topic G

106 User Interfaces and Desktops

Exam Objective (LX0–102)	Linux+ Powered by LPI Certification Lesson and Topic Reference
106.1 Install and configure X11	
• Verify that the video card and monitor are supported by an X server	Lesson 17 Topic E
• Awareness of the X font server	Lesson 18 Topic A
• Basic understanding and knowledge of the X Window configuration file	Lesson 17 Topic E
The following is a partial list of the used files, terms, and utilities:	
• /etc/X11/xorg.conf	Lesson 16 Topic B Lesson 18 Topic A
• xhost	Lesson 18 Topic A
• DISPLAY	Lesson 18 Topic A
• xwininfo	Lesson 18 Topic A
• xdpinfo	Lesson 18 Topic A
• X	Lesson 18 Topic A

Exam Objective (LX0–102)	Linux+ Powered by LPI Certification Lesson and Topic Reference
106.2 Setup a display manager	
• Turn the display manager on or off	Lesson 18 Topic A
• Change the display manager greeting	Lesson 18 Topic B
• Change default color depth for the display manager	Lesson 18 Topic A
• Configure display managers for use by X-stations	Lesson 18 Topic B
The following is a partial list of the used files, terms, and utilities:	
• /etc/inittab	Lesson 1 Topic D Lesson 18 Topic A
• xdm configuration files	Lesson 18 Topic B
• kdm configuration files	Lesson 18 Topic B
• gdm configuration files	Lesson 18 Topic B

Exam Objective (LX0–102)	Linux+ Powered by LPI Certification Lesson and Topic Reference
106.3 Accessibility	
• Keyboard Accessibility Settings (AccessX?)	Lesson 18 Topic D
• Visual Settings and Themes	Lesson 18 Topic D
• Assistive Technology (ATs)	Lesson 18 Topic D
The following is a partial list of the used files, terms, and utilities:	
• Sticky/Repeat Keys	Lesson 18 Topic D
• Slow/Bounce/Toggle Keys	Lesson 18 Topic D
• Mouse Keys	Lesson 18 Topic D
• High Contrast/Large Print Desktop Themes	Lesson 18 Topic D
• Screen Reader	Lesson 18 Topic D
• Braille Display	Lesson 18 Topic D
— Screen Magnifier	Lesson 18 Topic D
• On-Screen Keyboard	Lesson 18 Topic D
• Gestures (used at login, for example gdm)	Lesson 18 Topic D
• GOK	Lesson 18 Topic D
• emacspeak	Lesson 18 Topic D

107 Administrative Tasks

Exam Objective (LX0–102)	Linux+ Powered by LPI Certification Lesson and Topic Reference
107.1 Manage user and group accounts and related system files	
• Add, modify and remove users and groups	Lesson 2 Topic A Lesson 2 Topic C
• Manage user/group info in password/group databases	Lesson 2 Topic C
• Create and manage special purpose and limited accounts	Lesson 2 Topic A Lesson 2 Topic C Lesson 14 Topic B
The following is a partial list of the used files, terms, and utilities:	
• /etc/passwd	Lesson 2 Topic A
• /etc/shadow	Lesson 2 Topic A
• /etc/group	Lesson 2 Topic A
• /etc/skel	Lesson 2 Topic B

Exam Objective (LX0–102)	Linux+ Powered by LPI Certification Lesson and Topic Reference
107.1 Manage user and group accounts and related system files	
— chage	Lesson 2 Topic C
• groupadd	Lesson 2 Topic A
• groupdel	Lesson 2 Topic C
• groupmod	Lesson 2 Topic C
• passwd	Lesson 2 Topic A
• useradd	Lesson 2 Topic A
• userdel	Lesson 2 Topic C
• usermod	Lesson 2 Topic C

Exam Objective (LX0–102)	Linux+ Powered by LPI Certification Lesson and Topic Reference
107.2 Automate system administration tasks by scheduling jobs	
• Manage cron and at jobs	Lesson 10 Topic D
• Configure user access to cron and at services	Lesson 10 Topic D
The following is a partial list of the used files, terms, and utilities:	
• /etc/cron.{d,daily,hourly,monthly,weekly}	Lesson 10 Topic D
• /etc/at.deny	Lesson 10 Topic D
• /etc/at.allow	Lesson 10 Topic D
• /etc/crontab	Lesson 10 Topic D
• /etc/cron.allow	Lesson 10 Topic D
• /etc/cron.deny	Lesson 10 Topic D
• /var/spool/cron/*	Lesson 10 Topic D
• crontab	Lesson 10 Topic D
• at	Lesson 10 Topic D
• atq	Lesson 10 Topic D
• atrm	Lesson 10 Topic D

Exam Objective (LX0–102)	Linux+ Powered by LPI Certification Lesson and Topic Reference
107.3 Localization and internationalization	
• Locale settings	Lesson 10 Topic E

Exam Objective (LX0–102)	Linux+ Powered by LPI Certification Lesson and Topic Reference
107.3 Localization and internationalization	
• Timezone settings	Lesson 10 Topic E
The following is a partial list of the used files, terms, and utilities:	
• /etc/timezone	Lesson 10 Topic E
• /etc/localtime	Lesson 10 Topic E
• /usr/share/zoneinfo	Lesson 10 Topic E
• Environment variables: <ul style="list-style-type: none"> • LC_* • LC_ALL • LANG 	Lesson 10 Topic E
• /usr/bin/locale	Lesson 10 Topic E
• tzselect	Lesson 10 Topic E
• tzconfig	Lesson 10 Topic E
• date	Lesson 10 Topic E
• iconv	Lesson 10 Topic E
• UTF-8	Lesson 10 Topic E
• ISO-8859	Lesson 10 Topic E
• ASCII	Lesson 10 Topic E
• Unicode	Lesson 10 Topic E

108 Essential System Services

Exam Objective (LX0–102)	Linux+ Powered by LPI Certification Lesson and Topic Reference
108.1 Maintain system time	
• Set the system date and time	Lesson 10 Topic E
• Set the hardware clock to the correct time in UTC	Lesson 10 Topic E
• Configure the correct timezone	Lesson 10 Topic E
• Basic NTP configuration	Lesson 10 Topic E
• Knowledge of using the pool.ntp.org service	Lesson 10 Topic E
The following is a partial list of the used files, terms, and utilities:	
• /usr/share/zoneinfo	Lesson 10 Topic E
• /etc/timezone	Lesson 10 Topic E

Exam Objective (LX0–102)	Linux+ Powered by LPI Certification Lesson and Topic Reference
108.1 Maintain system time	
• /etc/localtime	Lesson 10 Topic E
• /etc/ntp.conf	Lesson 10 Topic E
• date	Lesson 10 Topic E
• hwclock	Lesson 10 Topic E
• ntpd	Lesson 10 Topic E
• ntpdate	Lesson 10 Topic E
• pool.ntp.org	Lesson 10 Topic E

Exam Objective (LX0–102)	Linux+ Powered by LPI Certification Lesson and Topic Reference
108.2 System logging	
• Syslog configuration files	Lesson 11 Topic B
• syslog	Lesson 1 Topic D
• standard facilities, priorities and actions	Lesson 11 Topic B
The following is a partial list of the used files, terms, and utilities:	
• syslog.conf	Lesson 11 Topic B
• syslogd	Lesson 11 Topic B
• klogd	Lesson 11 Topic B
• logger	Lesson 11 Topic B

Exam Objective (LX0–102)	Linux+ Powered by LPI Certification Lesson and Topic Reference
108.3 Mail Transfer Agent (MTA) basics	
• Create e-mail aliases	Lesson 13 Topic A
• Configure e-mail forwarding	Lesson 13 Topic A
• Knowledge of commonly available MTA programs (postfix, sendmail, qmail, exim) (no configuration)	Lesson 13 Topic A
The following is a partial list of the used files, terms, and utilities:	
• ~/.forward	Lesson 13 Topic A
• sendmail emulation layer commands	Lesson 13 Topic A
— newaliases	Lesson 13 Topic A

Exam Objective (LX0–102)	Linux+ Powered by LPI Certification Lesson and Topic Reference
108.3 Mail Transfer Agent (MTA) basics	
• mail	Lesson 13 Topic A
• mailq	Lesson 13 Topic A
• postfix	Lesson 13 Topic A
• sendmail	Lesson 13 Topic A
• exim	Lesson 13 Topic A
• qmail	Lesson 13 Topic A

Exam Objective (LX0–102)	Linux+ Powered by LPI Certification Lesson and Topic Reference
108.4 Manage printers and printing	
• Basic CUPS configuration (for local and remote printers)	Lesson 6 Topic A
• Manage user print queues	Lesson 6 Topic C
• Troubleshoot general printing problems	Lesson 16 Topic B
• Add and remove jobs from configured printer queues	Lesson 6 Topic C
The following is a partial list of the used files, terms, and utilities:	
• CUPS configuration files, tools and utilities	Lesson 6 Topic A
• /etc/cups	Lesson 6 Topic A
• lpd legacy interface (lpr, lprm, lpq)	Lesson 6 Topic A

109 Networking Fundamentals

Exam Objective (LX0–102)	Linux+ Powered by LPI Certification Lesson and Topic Reference
109.1 Fundamentals of internet protocols	
• Demonstrate an understanding network masks	Lesson 12 Topic A
• Knowledge of the differences between private and public “dotted quad” IPAddresses	Lesson 12 Topic A
• Setting a default route	Lesson 12 Topic B
• Knowledge about common TCP and UDP ports (20, 21, 22, 23, 25, 53, 80, 110, 119, 139, 143, 161, 443, 465, 993, 995)	Lesson 12 Topic A Lesson 13 Topic A

Exam Objective (LX0–102)	Linux+ Powered by LPI Certification Lesson and Topic Reference
109.1 Fundamentals of internet protocols	
• Knowledge about the differences and major features of UDP, TCP and ICMP	Lesson 12 Topic A
• Knowledge of the major differences between IPv4 and IPV6	Lesson 12 Topic A
The following is a partial list of the used files, terms, and utilities:	
• /etc/services	Lesson 12 Topic A
• ftp	Lesson 12 Topic A
• telnet	Lesson 13 Topic B
• host	Lesson 12 Topic C
• ping	Lesson 12 Topic A
• dig	Lesson 12 Topic C
• traceroute	Lesson 12 Topic B
• tracepath	Lesson 12 Topic B

Exam Objective (LX0–102)	Linux+ Powered by LPI Certification Lesson and Topic Reference
109.2 Basic network configuration	
• Manually and automatically configure network interfaces	Lesson 12 Topic A
• Basic TCP/IP host configuration	Lesson 12 Topic A
The following is a partial list of the used files, terms, and utilities:	
• /etc/hostname	Lesson 12 Topic A
• /etc/hosts	Lesson 12 Topic C
• /etc/resolv.conf	Lesson 12 Topic C
• /etc/nsswitch.conf	Lesson 12 Topic C
• ifconfig	Lesson 12 Topic A
— ifup	Lesson 12 Topic A
• ifdown	Lesson 12 Topic A
• route	Lesson 12 Topic B
• ping	Lesson 12 Topic A

Exam Objective (LX0–102)	Linux+ Powered by LPI Certification Lesson and Topic Reference
109.3 Basic network troubleshooting	
<ul style="list-style-type: none"> Manually and automatically configure network interfaces and routing tables to include adding, starting, stopping, restarting, deleting or reconfiguring network interfaces 	Lesson 12 Topic A
<ul style="list-style-type: none"> Change, view or configure the routing table and correct an improperly set default route manually 	Lesson 12 Topic B
<ul style="list-style-type: none"> Debug problems associated with the network configuration 	Lesson 16 Topic C
The following is a partial list of the used files, terms, and utilities:	
<ul style="list-style-type: none"> ifconfig 	Lesson 12 Topic A
<ul style="list-style-type: none"> ifup 	Lesson 12 Topic A
<ul style="list-style-type: none"> ifdown 	Lesson 12 Topic A
<ul style="list-style-type: none"> route 	Lesson 12 Topic B
<ul style="list-style-type: none"> host 	Lesson 12 Topic C
<ul style="list-style-type: none"> hostname 	Lesson 1 Topic B Lesson 9 Topic C
<ul style="list-style-type: none"> dig 	Lesson 12 Topic C
<ul style="list-style-type: none"> netstat 	Lesson 12 Topic B
<ul style="list-style-type: none"> ping 	Lesson 12 Topic A
<ul style="list-style-type: none"> traceroute 	Lesson 12 Topic B

Exam Objective (LX0–102)	Linux+ Powered by LPI Certification Lesson and Topic Reference
109.4 Configure client side DNS	
<ul style="list-style-type: none"> Demonstrate the use of DNS on the local system 	Lesson 12 Topic C
<ul style="list-style-type: none"> Modify the order in which name resolution is done 	Lesson 12 Topic C
The following is a partial list of the used files, terms, and utilities:	
<ul style="list-style-type: none"> /etc/hosts 	Lesson 12 Topic C
<ul style="list-style-type: none"> /etc/resolv.conf 	Lesson 12 Topic C
<ul style="list-style-type: none"> /etc/nsswitch.conf 	Lesson 12 Topic C

110 Security

Exam Objective (LX0–102)	Linux+ Powered by LPI Certification Lesson and Topic Reference
110.1 Perform security administration tasks	
• Audit a system to find files with the suid/sgid bit set	Lesson 5 Topic D
• Set or change user passwords and password aging information	Lesson 2 Topic C
• Being able to use nmap and netstat to discover open ports on a system	Lesson 12 Topic B Lesson 14 Topic E
• Set up limits on user logins, processes and memory usage	Lesson 14 Topic B
• Basic sudo configuration and usage	Lesson 14 Topic B
The following is a partial list of the used files, terms, and utilities:	
• find	Lesson 4 Topic B
• passwd	Lesson 2 Topic A
• lsof	Lesson 16 Topic A
• nmap	Lesson 14 Topic E
• chage	Lesson 2 Topic C
• netstat	Lesson 12 Topic B
• sudo	Lesson 14 Topic B
• /etc/sudoers	Lesson 14 Topic B
• su	Lesson 14 Topic B
• usermod	Lesson 2 Topic C
• ulimit	Lesson 14 Topic B

Exam Objective (LX0–102)	Linux+ Powered by LPI Certification Lesson and Topic Reference
110.2 Setup host security	
• Awareness of shadow passwords and how they work	Lesson 14 Topic B
• Turn off network services not in use	Lesson 12 Topic A
• Understand the role of TCP wrappers	Lesson 14 Topic A
The following is a partial list of the used files, terms, and utilities:	
• /etc/nologin	Lesson 1 Topic D
• /etc/passwd	Lesson 2 Topic A

Exam Objective (LX0–102)	Linux+ Powered by LPI Certification Lesson and Topic Reference
110.2 Setup host security	
• /etc/shadow	Lesson 2 Topic A
• /etc/xinetd.d/*	Lesson 13 Topic D
• /etc/xinetd.conf	Lesson 13 Topic B
• /etc/inetd.d/*	Lesson 13 Topic B
• /etc/inetd.conf	Lesson 12 Topic A
• /etc/inittab	Lesson 11 Topic A
• /etc/init.d/*	Lesson 11 Topic A
• /etc/hosts.allow	Lesson 14 Topic A Lesson 14 Topic B
• /etc/hosts.deny	Lesson 14 Topic B

Exam Objective (LX0–102)	Linux+ Powered by LPI Certification Lesson and Topic Reference
110.3 Securing data with encryption	
• Perform basic OpenSSH 2 client configuration and usage	Lesson 12 Topic D
• Understand the role of OpenSSH 2 server host keys	Lesson 12 Topic D
• Perform basic GnuPG configuration and usage	Lesson 7 Topic D Lesson 14 Topic A
• Understand SSH port tunnels (including X11 tunnels)	Lesson 12 Topic D
The following is a partial list of the used files, terms, and utilities:	
• ssh	Lesson 12 Topic D
• ssh-keygen	Lesson 12 Topic D
• ssh-agent	Lesson 12 Topic D
• ssh-add	Lesson 12 Topic D
• ~/.ssh/id_rsa and id_rsa.pub	Lesson 12 Topic D
• ~/.ssh/id_dsa and id_dsa.pub	Lesson 12 Topic D
• /etc/ssh/ssh_host_rsa_key and ssh_host_rsa_key.pub	Lesson 12 Topic D
• /etc/ssh/ssh_host_dsa_key and ssh_host_dsa_key.pub	Lesson 12 Topic D
• ~/.ssh/authorized_keys	Lesson 12 Topic D
• /etc/ssh_known_hosts	Lesson 12 Topic D

APPENDIX A

Exam Objective (LX0–102)	Linux+ Powered by LPI Certification Lesson and Topic Reference
110.3 Securing data with encryption	
• <code>gpg</code>	Lesson 7 Topic D Lesson 14 Topic A
• <code>~/.gnupg/*</code>	Lesson 14 Topic A

APPENDIX B

CompTIA Linux+ Powered by LPI: Acronyms and Abbreviations

Introduction

The following is a list of acronyms and abbreviations that appear in the CompTIA Linux+ exam powered by LPI. Candidates are encouraged to review the complete list and attain a working knowledge of all listed acronyms and abbreviations as part of a comprehensive exam preparation program.

Acronym/ Abbreviation	Associated Term
ACL	Access Control List
ASCII	American Standard Code for Information Interchange
APT	Advanced Package Tool
ARP	Address Resolution Protocol
BASH	Bourne Again Shell
BIND	Berkeley Internet Naming Daemon
BIOS	Basic Input/Output System
CD	Compact Disc
CA	Certificate Authority
CLI	Command Line Interface
CGI	Common Gateway Interface
CUPS	Common Unix Printing System
CPU	Central Processing Unit
CNAME	Canonical Name
CHAP	Challenge Handshake Authentication Protocol
CMOS	Complementary Metal Oxide Semiconductor

APPENDIX B

Acronym/ Abbreviation	Associated Term
DAC	Discretionary Access Control
DES	Data Encryption Standard
DHCP	Dynamic Host Control Protocol
DMA	Direct Memory Address
DNS	Domain Name System
DVD	Digital Versatile Disc
ESMTP	Extended SMTP
EHLO	Extended HELLO
FAT	File Allocation Table
FTP	File Transfer Protocol
FHS	Filesystem Hierarchy Standard
FQDN	Fully Qualified Domain Name
FIPS	First nondestructive Interactive Partition Splitting program
GB	Gigabyte
GUI	Graphical User Interface
GDM	GNOME Display Manager
GNU	GNU is not Unix
GMT	Greenwich Mean Time
GPG	GNU Privacy Guard
GRUB	Grand Unified Bootloader
GPL	General Public License
GCC	GNU Compiler Collection
GUI	Graphical User Interface
HAL	Hardware Abstraction Layer
HDD	Hard Disk Drive
HTTP	Hyper Text Transfer Protocol
HTTPD	Hyper Text Transfer Protocol Daemon
HTTPS	Hyper Text Transfer Protocol-Secure
IMAP	Internet Message Access Protocol
IDS	Intrusion Detection System
ISC	Internet Software Consortium
ISO	International Organization for Standardization
IRQ	Interrupt ReQuests
ICMP	Internet Control Message Protocol
IMAP	Internet Message Access Protocol
KDM	KDE Display Manager
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LV	Logical Volumes
LED	Light Emitting Diode

Acronym/ Abbreviation	Associated Term
LVM	Logical Volume Manager
LPD	Line Printer Daemon
LMTP	Local Mail Transport Protocol
MAC	Mandatory Access Control
MAN	Metropolitan Area Network
MB	Megabyte
MBR	Master Boot Record
MDA	Mail Delivery Agent
MRA	Mail Retrieval Agent
MTA	Mail Transfer Agent
MUA	Mail User Agent
MX	Mail Exchanger
MSP	Message Send Protocol
MIME	Multipurpose Internet Mail Extensions
NFS	Network File System
NIC	Network Interface Card
NAS	Network Access Server
NNTP	Network News Transfer Protocol
NTFS	New Technology File System
NTP	Network Time Protocol
OS	Operating System
PAP	Password Authentication Protocol
PKC	Public Key Cryptography
PRNG	Pseudo Random Number Generation
PHP	Personal Home Pages
PID	Process ID
POP	Post Office Protocol
PPID	Parent Process ID
PPP	Point to Point Protocol
PDL	Page Description Language
PPD	PostScript Printer Definitions
POST	Power-On Self Test
RADIUS	Remote Authentication Dial-in User Services
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
RDBMS	Relational Database Management System
RDP	Remote Desktop Protocol
RHEL	Red Hat Enterprise Linux
RMON	Remote Monitoring
RPM	RedHat Package Manager

APPENDIX B

Acronym/ Abbreviation	Associated Term
RTC	Real Time Clock
RJE	Remote Job Entry
RFC	Request for Comments
SASL	Simple Authentication and Security Layer
SOA	Start Of Authority
SCI	System Call Interface
SCP	Secure Copy
SCSI	Small Computer System Interface
SELinux	Security-Enhanced Linux
SFTP	Secure File Transfer Protocol
SH	Shell
SMTP	Simple Mail Transport Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Securer Socket Layer
SSID	Service Set Identifier
SUID	Set User ID
SGID	Set Group ID
SMB	Server Message Block
STDIN	Standard Input
STDOUT	Standard Output
STDERR	Standard Error
SFTP	Simple File Transfer Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TTL	Time to Live
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
UID	User ID
USB	Universal Serial Bus
UID	User ID
UPG	User Private Group
UPS	Uninterrupted Power Supply
UTC	Universal Time Coordinated
VG	Volume Group
VFAT	Virtual File Allocation Table
VNC	Virtual Network Computing
VGDA	Volume Group Descriptor Area
WAN	Wide Area Network
YUM	Yellow dog Updater, Modified

APPENDIX C

Syntax

Introduction

The following is a list of the most frequently used commands with their syntax. Candidates are encouraged to review the complete list and attain a working knowledge of all listed commands as a part of a comprehensive exam preparation program.

Command	Syntax
alias	alias {command}='{command} [options]'
apropos	apropos {keyword}
apt-get	apt-get [options] {command}
aspell	aspell [options]
at	at [options] {time}
awk	awk [options] {file}
bg	bg {%#}
bunzip2	bunzip2 {file name}
bzcat	bzcat {file name}
bzdiff	bzdiff {file name}
bzip2	bzip2 {file name}
bzip2recover	bzip2recover {file name}
bzless	bzless {file name}
bzmore	bzmore {file name}
cal	cal {month} {year}
cancel	cancel [command options]
cat	cat [command options] {file name}
cd	cd {absolute or relative path}

APPENDIX C

Command	Syntax
cp	cp [<i>command options</i>] { <i>absolute or relative path of the file or directory to be copied</i> }/{ <i>file or directory name</i> } { <i>absolute or relative path of the destination</i> }
chown	chown { <i>user name</i> } { <i>file name</i> } OR chown { <i>user name.group name</i> } { <i>file name</i> } OR chown { <i>user name.</i> } { <i>file name</i> } OR chown { <i>.group name</i> } { <i>file name</i> }
chattr	chattr [-RV] [-v <i>version</i>] { <i>mode</i> } <i>files</i>
command --help	command - <i>options</i>
count	operator [<i>count</i>] { <i>motion</i> }
chmod	chmod [<i>option</i>] { <i>mode</i> } { <i>file name</i> }
createrepo	createrepo [<i>options</i>] < <i>directory</i> >
cron	cron [<i>option</i>] { <i>mail command</i> }
chgrp	chgrp { <i>group</i> } { <i>file name</i> }
chkconfig	chkconfig [<i>option</i>] { <i>service name</i> } { <i>on/off/reset</i> }
cp	cp [<i>options</i>] { <i>absolute or relative path of the file or directory to be copied</i> }/{ <i>file or directory name</i> } { <i>absolute or relative path of the destination</i> }
date	date +[<i>format</i>]
dd	dd [<i>operand</i>]... OR dd [<i>option</i>]
dump	dump {-level #} { <i>dump file</i> } { <i>filesystem/file/directory</i> }
date	date +[<i>format</i>]
dumpe2fs	dumpe2fs [<i>options</i>] { <i>block size</i> } { <i>device name</i> }
diff	diff { <i>file name 1</i> } { <i>file name 2</i> }
dig	dig [<i>command options</i>] { <i>query options</i> } { <i>Fully Qualified Domain Name IP address</i> }
dpkg	dpkg [<i>option</i>] { <i>action</i> }
echo	echo {" <i>string</i> "}
e2fsck	e2fsck /dev/{ <i>filesystem</i> }
e2label	e2label /dev/{ <i>device name</i> } { <i>partition number</i> }
export	export <i>variable</i>
finger	finger [<i>user name</i>]
fdisk	fdisk [<i>option</i>] { <i>device name</i> }
fg	fg { <i>%#</i> }

Command	Syntax
fsck	fsck -t {filesystem type} [options] OR fsck -r /dev/{filesystem}
find	find [options] {search locations} {search criteria} {actions}
file	file [options] {file name}
ftp	ftp [command options] {hostname}
gzip	gzip [command options] {file name}
groupdel	groupdel {group name}
groupmod	groupmod [-g gid [-o]] [-n new group name] [old group name]
groupadd	groupadd [options] {group name}
parted	parted [option] device {command [argument]}
grep	grep [command options] {keyword} {file name}
gpg	gpg [options] {command} {arguments}
groupadd	groupadd {group name}
groupdel	groupdel {group name}
groupmod	groupmod -g {GID}
history	history [options]
host	host [command options] {FQDN IP address}
hostname	hostname [options] {hostname}
inetd	inetd [option] [configuration file]
info	info {command}
insmod	insmod {file name} {module options}
ifconfig	ifconfig {interface name} {options or address}
ip	ip [options] {object} {command help}
iwconfig	iwconfig {interface name} {options or address}
iptables	iptables [-t table] {commands} {chain/rule specification} [options/parameters]
ls	ls [options] [absolute or relative path of the directory]
kill	kill [signal option] {PID}
killall	killall [signal option] {command}
klogd	klogd [options]
last	last [options]
lastlog	lastlog [options]
lp	lp [command options] {file name}

APPENDIX C

Command	Syntax
ln	ln [option] [-T] {target link name}
ls	ls [command options] [absolute or relative path of the directory]
logrotate	logrotate [options] {configuration file}
lsmod	lsmod
lpr	lpr [command options] {file name}
lpq	lpq [command options] {print queue name}
lprm	lprm {print job id}
lpc	lpc [parameter]
lpstat	lpstat [command options]
links	links [options] {URL}
lsattr	lsattr [-RVadv] [files...]
locate	locate [options] {string}
mv	mv {absolute or relative path}/{file or directory name} {absolute or relative path}/{new file or directory name}
modinfo	modinfo {module options}
man	man topic
mkinitrd	mkinitrd [options] {image name} {kernel version}
mkfs	mkfs [options] {filesystem}
mke2fs	mke2fs [options] {filesystem name}
mkdir	mkdir {directory name}
mount	mount [options] {device} {mountpoint}
mkswap	mkswap [option] device {size}
modprobe	modprobe [option] {module name}
mknod	mknod [option]... {name} {type} [major minor]
md5sum	md5sum --check {file name}
make	make {key file digital certificate}
mdadm	mdadm {mode} {raid device} [options] {component devices}
mv	mv {absolute or relative path}/{file or directory name} {absolute or relative path}/{new file or directory name}
netstat	netstat [options]
nice	nice -n {priority} {command}
nohup	nohup {command}
nslookup	nslookup {host name or FQDN}

Command	Syntax
nmap	nmap [scan type] [options] {target specification}
openssl	openssl {command} [options] {arguments}
parted	parted [option] device {command [argument]}
partprobe	partprobe [options] [device]
pr	pr [command options] {file name}
passwd	passwd [user name]
pwd	pwd [option]
ps	ps [options]
pstree	pstree [options]
pidof	pidof [command options] {string}
pgrep	pgrep [command options] {process name}
pkill	pkill [signal option] {command}
popd	popd [options]
pushd	pushd [options] {directory name}
renice	renice {priority} [options]
restore	restore [options] {file}
rm	rm [command options] {absolute or relative path of file or directory}/{file or directory name}
rmdir	rmdir {directory name}
rpm -q	rpm -q {what_packages} {what_information}
rpm -V	rpm -V package_name
rndc	rndc [rndc options] {rndc command}
rsync	rsync {source file or folder} {destination file or folder}
rdesktop	rdesktop [options] server[:port]
service	service {service name} {options}
sleep	sleep {time}
shutdown	shutdown [-t seconds] [-options] time [warning message]
sfdisk	sfdisk [options] device
swapon	swapon -e OR swapon -a
swapoff	swapoff -a
sysctl	sysctl [command options] {kernel parameter}={value}
syslogd	syslogd [options]
system-config-services	system-config-services

APPENDIX C

Command	Syntax
ssh-keygen	ssh-keygen <i>[options]</i>
sed	sed 'address/pattern/action' file name
smbclient	smbclient //machine/service
sftp	sftp hostname
shasum	shasum --check {file name}
sudo	sudo command-name command-options
tail	tail <i>[options]</i> {file name}
tar	tar <i>[archiving command options]</i> {destination file}.tar {source directory}
tee	tee <i>[options]</i> {file}
test	test {expressions}
telinit	telinit {runlevel}
top	top <i>[options]</i>
tr	tr {'character 1'} {'character 2'} < {file name}
traceroute	traceroute <i>[options]</i> {hostname/ip address}
touch	touch {file name}
tune2fs	tune2fs <i>[options]</i> {device name}
tmpwatch	tmpwatch <i>[options]</i> {hours}
tcpdump	tcpdump <i>[option]</i> {expression}
uname	uname <i>[options]</i>
uptime	uptime OR uptime [-V]
useradd	useradd <i>[command options]</i> {user name}
userdel	userdel <i>[command options]</i> {user name}
usermod	usermod <i>[command options]</i> {user name}
umount	umount <i>[options]</i> {directory/device}
uniq	uniq <i>[command options]</i> {file name}
unzip	unzip <i>[command options]</i> {file name}
umask	umask number
vim	vim <i>[options]</i> {file}
vncserver	vncserver {:display number} {-option}
vncviewer	vncviewer <i>[options]</i> {hostname/ipaddress}{:display}
w	w <i>[options]</i> {user name}
wc	wc <i>[command options]</i> {file name}
vim	vim {file name}

Command	Syntax
whatis	<code>whatis <i>command</i></code>
which	<code>which {<i>file name</i>}</code>
whereis	<code>whereis [-bmsu] [-BMS <i>directory...</i> -f] <i>file name ...</i></code>
who	<code>who [<i>options</i>]</code>
whoami	<code>whoami [<i>option</i>]</code> ...
wireshark	<code>wireshark [<i>options</i>]</code>
wget	<code>wget [<i>command options</i>] http://{<i>hostname or IP of the destination</i>}</code>
xargs	<code>xargs [<i>options</i>] {<i>commands</i>}</code>
yum	<code>yum [<i>options</i>] {<i>command</i>} {<i>package name</i>}</code>
yumdownloader	<code>yumdownloader [<i>options</i>] {<i>package name</i>}</code>

LESSON LABS

Due to classroom setup constraints, some labs cannot be keyed in sequence immediately following their associated lesson. Your instructor will tell you whether your labs can be practiced immediately following the lesson or whether they require separate setup from the main lesson content. Lesson-level lab setup information is listed in the front of this manual in the course setup section.

LESSON 1 LAB 1

Discussing the Evolution of Linux

Scenario:

You are preparing a presentation on the evolution and benefits of Linux. You decide to initiate a discussion about the advantages of using Red Hat Enterprise Linux as the operating system for all the users in the organization.

1. What are the benefits of releasing software under GPL?

2. Identify the advantages of using open source software.

3. Compare free software and proprietary software.

4. List the features of Linux that make it competitive as an operating system.
-
-

LESSON 1 LAB 2

Performing Basic Tasks in Linux



You can find a suggested solution for this activity in the Lesson 1 Lab 2 solution.html file in the Familiarizing_Linux\Solution folder in the student data files.

Before You Begin:

Ensure that you are logged in as the root user to perform all lesson lab activities.

Scenario:

You recently joined Our Global Company (OGC) and are required to prepare a report on the Linux system for which you need to determine how long the server is running and the number of users who use the system.

1. Check the uptime of the Linux system.
 2. Determine the users currently logged in to the system.
 3. Check the login and logout details of the Linux system for the last month.
 4. Check the details of the failed logins.
-
-

LESSON 2 LAB 1

Managing User and Group Settings



You can find a suggested solution for this activity in the Lesson 2 Lab 1 solution.html file in the Managing_Users_and_Groups\Solution folder in the student data files.

Scenario:

A contract employee, Mike, joined your organization. You need to create a user account for him based on the following details:

- Username: contractor01
- Password: myp@\$w0rd
- Period until which the user account needs to be valid: November 16, 2011
- The directory to be set as the default home directory: /home/oncontract/contractor01
- Group to which the new user needs to belong: Contract

-
1. Create a user account, contractor01, and configure the user profile.
-
2. Modify the password expiration settings.
-
3. Create a group, Contract, and add the user, contractor01, to it.
-
-

LESSON 3 LAB 1

Managing Partitions



You can find a suggested solution for this activity in the Lesson 3 Lab 1 solution.html file in the Managing_Partitions\Solution folder in the student data files.

Scenario:

As a system administrator, you will need to set up systems for new employees. You are required to configure their hard disks and separate the user accessible areas on the disk from the sensitive ones that contain system and software information. You must also populate the partitions with filesystems and ensure easy identification of the partitions. The users' requirements are as follows:

Size of partition usr: 1024 MB

Size of partition root: 1024 MB

You are also required to create a filesystem labeled company policies and place it in the usr partition.

-
1. Create partitions.
 2. Create two logical partitions within the extended partition.
 3. Set the ext2 filesystem for the logical partitions.
 4. Verify that the new partitions have the ext2 filesystem.
 5. Apply a label to the first logical partition that was created.
 6. Verify the label applied to the partition.
 7. Mount the partition using its label.
-
-

LESSON 3 LAB 2

Organizing Files in Linux



You can find a suggested solution for this activity in the Lesson 3 Lab 2 solution.html file in the Managing_Partitions\Solution folder in the student data files.

Data Files:

- Software_Rules.txt
- Hardware_Inventory.txt

Before You Begin:

Ensure that the required data files are copied into the /root directory.

Scenario:

As the junior administrator of your organization, you are required to perform the following tasks:

- Move the Software_Rules.txt file from the /root directory to the /home directory.
- Copy the Hardware_Inventory.txt file from the /root directory to the /home directory.
- Remove the Hardware_Inventory.txt file from the /root directory.
- Set the Nautilus Browser to open in spatial mode.

-
1. Move the Software_Rules.txt file to the /home directory.
-
2. Copy the Hardware_Inventory.txt file into the /home directory.
-
3. Remove the Hardware_Inventory.txt file from the /root directory.
-
4. Change the Nautilus Browser's view from spatial mode to browser mode.
-
-

LESSON 4 LAB 1

Finding Files



You can find a suggested solution for this activity in the Lesson 4 Lab 1 solution.html file in the Managing_Files\Solution folder in the student data files.

Scenario:

You work on a multiuser system and you want to search for files you own, which are located in different directories on the system. You regularly back up important files and directories on your system. You also want to locate unnecessary files and directories that are more than two years old so that you will be able to delete them later.

1. Open the GNOME search tool and search for files owned by the root user.
 2. Refine the search to include only empty files owned by the root user.
 3. Refine the search to include only empty files owned by the root user that are older than 730 days.
-
-

LESSON 4 LAB 2

Managing Files in Linux



You can find a suggested solution for this activity in the Lesson 4 Lab 2 solution.html file in the Managing_Files\Solution folder in the student data files.

- Leave_Log.txt
- Hardware_Report_09.txt
- Empclaimfeb.txt
- Empclaimjan.txt
- Policies.txt

Before You Begin:

Ensure that the required data files are copied into the /root directory.

Scenario:

You want to clean up unused files in your Linux system. Before the clean up, you decide to archive important work-related files and create links to those files in the root directory.

1. Remove the Leave_Log.txt file from your home directory.
2. Create a zip archive of the Empclaimfeb.txt, Empclaimjan.txt, and Policies.txt files in your home directory.
3. Create a hard link for the Hardware_Report_09.txt file in the / directory.

LESSON 5 LAB 1

Modifying File Permissions and Ownership



You can find a suggested solution for this activity in the Lesson 5 Lab 1 solution.html file in the Linux_Permissions\Solution folder in the student data files.

- Leave_Log.txt
- Stationery_List.txt

Before You Begin:

Ensure that the required data files are copied in the /root directory.

Scenario:

As a junior system administrator, you are responsible for managing user permissions for the administration team. In this role, you need to perform the following tasks:

1. Audit on the number of existing users and groups on the system.
2. Change the permissions of certain files.

1. View the users and groups on your Linux system.
2. Modify the permission of the Leave_Log.txt file to be read-only for all users.
3. Modify the permission using the character method and verify the change.
4. Modify the permission of the Stationery_List.txt file, in the Nautilus browser, to be writable by all users by using the **Properties** dialog box.

LESSON 5 LAB 2

Working with Permissions and Ownership

Scenario:

In this activity, you will assess the knowledge that you gained in this lesson.

1. Which binary value allows you to assign read, write, and execute permissions to a file?
 - a) 4
 - b) 2
 - c) 7
 - d) 6

2. True or False? Only the owner of the file can change the permissions for a file or directory.
☐ True
☐ False

3. Which option represents the default base permissions for nonexecutable files in Linux?
 - a) 777
 - b) 644
 - c) 666
 - d) 744

4. True or False? For directories created by the root user, the default permission is 644.
☐ True
☐ False

5. True or False? The numbers given with the umask command specify the permissions that need to be cleared from the default settings.
☐ True
☐ False

6. Chris needs to recursively change the ownership of files through a directory structure. Which option of the chown command will allow Chris to do so?
 - a) -c
 - b) -R
 - c) -v
 - d) -f

7. Which statements about sticky bits are true? Select all that apply.
- a) Any user can delete the file or directory with a sticky bit.
 - b) A sticky bit is a permission bit that provides protection for files in a directory.
 - c) A sticky bit on a file indicates to the operating system that the file will be frequently executed.
 - d) A sticky bit closes a program or file so that it needs to be reloaded when it is invoked again.
-
8. True or False? ACL allows the assignment of permissions to individual users or groups even if they do not belong to the owner's group or the owning group.
- ☐ True
- ☐ False
-
9. True or False? By default, system processes are usually owned by the root user.
- ☐ True
- ☐ False
-
-

LESSON 6 LAB 1

Configuring Printer Settings



You can find a suggested solution for this activity in the Lesson 6 Lab 1 solution.html file in the Printing_Files/Solution folder in the student data files.

Data Files:

- Onsite_Training_Policy.txt

Before You Begin:

1. If necessary, connect the USB printer to the system. Ensure that the necessary drivers are downloaded and the printer is ready for use.
2. Copy the required data file into the /root directory.

Scenario:

You have been transferred on-site for training. You want to configure a printer for your laptop, which is running the Linux operating system. In addition, you want to apply text formatting and print the training policy document.

-
1. Configure a generic Postscript printer on srvB.
-
2. Select the make and model of the printer to be configured.
-

3. Check whether **printer2** has been added to the **Local Printers** list and make it the default printer of your system.
 4. Apply text formatting on Onsite_Training_Policy.txt to print 30 lines per page.
 5. Preview the document after specifying a header "The Onsite Training Policy" and applying double-spacing for the document.
-
-

LESSON 6 LAB 2

Printing Files in Linux

Scenario:

In this activity, you will examine how to print files in Linux.


1. Which statements about CUPS are true? Select all that apply.
 - a) CUPS is a systematic print management system for Linux that allows a computer to function as a print server.
 - b) CUPS can process only a single data format on the same print server.
 - c) CUPS is designed for scheduling print jobs, processing administrative commands, and providing printer status information to local and remote programs.
 - d) A system running CUPS is a host that can initiate print jobs from client systems.
 2. Which statements about print queues are true? Select all that apply.
 - a) Print queues are used by the print daemon so that applications that need to use the printer have to wait for the current print job to complete before issuing the command for printing.
 - b) Print queues allow multiple users to share a printer.
 - c) A print queue is a storage area that sorts outgoing print jobs.
 - d) Print queues contain a list of print jobs with details of the file being printed and the files yet to be printed.
 3. True or False? If a printer is busy, each job is placed in a waiting line, or print queue, and stored in a temporary storage space called a print spool.
☐ True
☐ False
-

4. Which command allows you to start or stop a printer, enable or disable queues, manage jobs in the queue, and obtain a status report on the printers and queues?
- a) lpr
 - b) lpq
 - c) lpc
 - d) lprm
-
5. You want to preview a document with double spacing using the pr command. Which option should you use?
- a) -d
 - b) -m
 - c) -l
 - d) -h
-
6. True or False? The lp command sends data directly to the printer.
- ☐ True
- ☐ False
-
7. Which statements about Samba are true? Select all that apply.
- a) Samba is a suite of network sharing tools that help in the sharing of files and printers on a network, which consists of computers running on different operating systems.
 - b) Samba is an open source software application that provides enhanced interoperability with better performance and minimal maintenance.
 - c) Samba uses the SMB protocol to enable Linux systems to communicate with computers running on other operating systems and share network resources such as printers.
 - d) Samba is a suite of network sharing tools that help in the sharing of files and printers on a network, which consists of computers running on homogeneous operating systems.
-
8. Which command allows you to use a remote printer by copying a file to the remote spool directory where it waits until the remote print server can print it?
- a) lprm
 - b) lpr
 - c) lpq
 - d) lpc
-
9. True or False? Samba provides enhanced network security by allowing Active Directory (AD) support.
- ☐ True
- ☐ False
-

10. True or False? The `/etc/hosts.lpd` file lists the names of the remote computers that can use a local printer.
- ☐ True
 - ☐ False
-
-

LESSON 7 LAB 1

Managing Packages

 You can find a suggested solution for this activity in the Lesson 7 Lab 1 solution.html file in the Managing_Packages\Solution folder in the student data files.

Before You Begin:

1. Ensure that all the five CDs of the RHEL 5.3 installation are available.
2. Perform the steps on `srvA`. To perform this lab on `srvB`, you need to configure the yum package manager to disable `gpgcheck`.

Scenario:

You are assigned the task of managing a few systems on the network. You need to update all the systems with gimp packages. You decide to set up a centralized repository.

-
1. Copy installation files from all the five setup discs to the `/setup` directory.
 2. Define the `/setup` directory as a private repository.
 3. Install gimp packages using the YUM package manager.
-
-

LESSON 7 LAB 2

LESSON LABS

Working with Packages

Scenario:

In this activity, you will examine working with packages.

1. Which package manager does Red Hat Linux use?
 - a) Red Hat Package Assistance
 - b) DEB
 - c) Red Hat Package Manager (RPM) or RPM Package Manager
 - d) apt-get

 2. True or False? The `rpm -e` command is used to remove a Red Hat package.
☐ True
☐ False

 3. True or False? Packages include all the files required to run an application.
☐ True
☐ False

 4. True or False? To repair a package, you must first uninstall it and then reinstall it.
☐ True
☐ False

 5. True or False? If you perform a package update and the package is not already installed on the system, it will be not be installed.
☐ True
☐ False

 6. Janet, a junior administrator, wants to create a repository by using a local directory. But, she does not want to include all the files in the directory. Which command allows her to achieve this?
 - a) `createrepo -x`
 - b) `createrepo -p`
 - c) `createrepo -h`
 - d) `createrepo -c`
-

7. Pat, a software engineer, wants to select the checksum to be used while creating a repository. Which command does he have to use?
- a) createrepo -x
 - b) createrepo -s
 - c) createrepo -h
 - d) createrepo -c
-
8. True or False? Repositories contain only the source code for packages.
- ☐ True
 - ☐ False
-
9. Robert, a system administrator, wants to view the version, dependencies, and integrity of a specific package using the dpkg command. Which option must he specify to get the desired output?
- a) -L
 - b) -p
 - c) -l
 - d) -S
-
10. Which statements about makefile are true?
- a) makefile contains the details of files, dependencies, and rules with which an executable application is built.
 - b) makefile is used to configure and compile driver and install application.
 - c) System built-in rules for maintaining, updating, and regenerating groups of programs are overridden by the contents of makefile.
 - d) System built-in rules for maintaining, updating, and regenerating groups of programs are not overridden by the contents of makefile.
-
-

LESSON 8 LAB 1

Exploring the Kernel Services and Configuration



You can find a suggested solution for this activity in the Lesson 8 Lab 1 solution.html file in the Managing_Kernel_Services\Solution folder in the student data files.

Before You Begin:

Copy the grub.conf file as grub.conf.bak to make a backup of the grub.conf file.

Scenario:

The system administrator is responsible for monitoring the performance of kernels to ensure smooth running of the systems. Therefore, you decide to acquaint yourself with various kernel services and how to configure them.

-
1. Create a new initrd image.
 2. Update the GRUB configuration with the new initrd image.
 3. View the new initrd image and boot the system using it.
 4. View all the peripheral devices that are connected to the system.
 5. View all the hardware devices that are connected to the system using the HAL device manager.
 6. Monitor the processes currently running on the system.
-
-

LESSON 8 LAB 2

Managing the Linux Kernel

Scenario:

In this activity, you will examine how to manage the Linux kernel.

1. Which is not a core function of the Linux kernel?
 - a) Filesystem access
 - b) Resource allocation
 - c) Management of processes
 - d) Network communication

2. What function does the device management layer of the Linux kernel perform?
 - a) Enables the kernel to schedule and process function calls.
 - b) Controls interfacing between user applications and hardware devices.
 - c) Manages the computer's memory.
 - d) Allocates separate execution space on the processor for running processes.

3. What function does the SCI layer of the Linux kernel perform?
 - a) Handles function calls
 - b) Controls device access
 - c) Organizes data
 - d) Allocates execution space for processes on the processor

4. Which statements about the Linux kernel are true? Select all that apply.
 - a) In a modular kernel, all the modules are built-in.
 - b) A monolithic kernel can interact faster with devices than a modular kernel.
 - c) A monolithic kernel utilizes less RAM.
 - d) A modular kernel is also known as a micro kernel.
 - e) A monolithic kernel is also known as a dynamic kernel.

5. Anne, a Linux programmer, wants to install a specific module in the currently running kernel. Which utility should she use?
 - a) insmod
 - b) modinfo
 - c) lsmod
 - d) modprobe

6. Diana, an administrator trainee, wants to view all the current kernel parameter values in a tabular format. Which sysctl command option should she use?
 - a) -n
 - b) -P
 - c) -a
 - d) -A

7. Peter, a system programmer, wants to load a module in the initrd image before the loading of SCSI modules. Which mkinitrd command option should he use?
 - a) --builtin={module name}
 - b) --fstab={fstab}
 - c) --preload={module name}
 - d) --fstab={module name}


8. Which special device provides unlimited null characters for writing onto any program or file?
 - a) /dev/null
 - b) /dev/zero
 - c) /dev/random
 - d) /dev/null/random

9. Which special device does not provide any data to a program or file?
 - a) /dev/null
 - b) /dev/zero
 - c) /dev/zero/random
 - d) /dev/zero/urandom

10. Pam wants to view the list of devices connected to her system in text mode. Which utility should she use?
 - a) hal-devices-manager
 - b) hal-device
 - c) hal-devices
 - d) hal-device-manager

LESSON 9 LAB 1

Managing Files Using Basic Bash Shell Operations

 You can find a suggested solution for this activity in the Lesson 9 Lab 1 solution.html file in the Working_with_Bash_and_Shell_scripts\Solution folder in the student data files.

- Software_List.txt
- Software_Rules.txt
- Software_Audit_Report_08.txt
- Software_Audit_Report_09.txt

Before You Begin:

Ensure that the required data files are copied into the /root directory.


Scenario:

You want to search for documents that you created several months ago. You remember that the names of the files begin with the word “Software.” You want to find them and create a backup of the files in the /mybackup directory.

-
1. Search for file names beginning with “Software.”
-
2. Create a backup of the files in the /mybackup directory.
-
-

LESSON 9 LAB 2

Using Variables to Configure the Shell Environment

 You can find a suggested solution for this activity in the Lesson 9 Lab 2 solution.html file in the Working_with_Bash_and_Shell_scripts\Solution folder in the student data files.

Scenario:


Your colleague asked you to set up his Linux system with the following requirements.

- Write a script to remind him to fill the effort tracking sheet everyday.
- Assign the /root directory to the local path in the system.
- The command prompt should reflect the company name, “Our Global Company.”
- Customize the history file size to display only 500 entries on running the `history` command.

-
1. Write a script named `Reminder` to remind the user to fill his effort tracking sheet whenever he logs in.
-
2. Save and convert the file into an executable script.
-
3. Test the script.
-
4. Customize the environment variables in the `~/.bashrc` script file to suit your colleague’s needs.
-
5. Check the changes.
-
-

LESSON 9 LAB 3

Applying Basic Scripting Techniques

 You can find a suggested solution for this activity in the Lesson 9 Lab 3 solution.html file in the Working_with_Bash_and_Shell_scripts\Solution folder in the student data files.


Scenario:

You want to track your daily tasks so that you can fill your weekly timecard easily. You decide to maintain a list, daily work-done, in a text file with unique names. You decide to name each file with the current date and add the date as the first line of each file. You want to write a script named dailyupdate to automate this process.

1. Create a script file named dailyupdate using Vim.
 2. Write the code to create text files redirecting the date input from the user.
 3. Write the code to confirm file creation with a unique file name.
 4. Test the script.
-
-

LESSON 10 LAB 1

Performing Process Management

 You can find a suggested solution for this activity in the Lesson 10 Lab 1 solution.html file in the Managing_Jobs_and_Processes\Solution folder in the student data files.

Scenario:

As a system administrator, you have to monitor the processes running on your system and their usage of system resources. You will perform the following tasks everyday.

- List all background jobs.
- Suspend or terminate unnecessary processes.

1. Execute three commands as background processes.
 2. Terminate the last job.
-

3. Bring the second job to the foreground and suspend it.
 4. View the list of processes running in the background.
 5. View the current running processes and all other running processes.
-
-

LESSON 10 LAB 2

Multitasking in Linux



You can find a suggested solution for this activity in the Lesson 10 Lab 2 solution.html file in the Managing_Jobs_and_Processes\Solution folder in the student data files.


Scenario:

You received several complaints about processes taking longer time than usual to complete. There are certain commands that are running with high priority, which can be lowered. Practice altering the command priority and delaying jobs to run at different times. This should free up some processing power so that critical processes can be run.

-
1. View the processes on your system.
 2. Issue the command to copy installation files as a background process.
 3. Renice the copy process by using the `top` command.
 4. Issue a command to run in the background and log out of the system.
 5. Log in as root and verify that the job is complete.
-
-

LESSON 11 LAB 1

Configuring System Services

 You can find a suggested solution for this activity in the Lesson 11 Lab 2 solution.html file in the Configuring_System_Services\Solution folder in the student data files.

Scenario:

You are a system administrator in OGC systems. Your organization has many branches and has already enabled system and network services on the server to allow employees from different branches to communicate and share information. You need to monitor the activities that take place on the server.

1. Enable SELinux on the system.
 2. Configure syslogd to set up the system to act as a central network log server.
 3. Configure alerts and warning on logs.
-
-

LESSON 11 LAB 2

Managing System Services

Scenario:

In this activity, you will examine system services.

1. Identify the syntax of the chkconfig command.
 - a) `chkconfig [option] {service name} {on|off|reset}`
 - b) `chkconfig [option] {on|off|reset} {service name}`
 - c) `chkconfig [option] {on|off|reset}`
 - d) `chkconfig {service name}`
-

2. Steve, a system administrator, wants to perform automatic rotation of logs on his system. Which utility should he use?
 - a) rotate
 - b) logrotate
 - c) autologrotate
 - d) rotatelog
 - e) syslogd

3. Ruby, a network administrator, wants the syslogd utility to receive messages from a network. Which syslogd command option should she use?
 - a) -r
 - b) -d
 - c) -D
 - d) -m

4. Which utility tracks kernel messages by prioritizing them?
 - a) klogd
 - b) syslogd
 - c) syslog
 - d) lastlog

5. Jane, a Linux programmer, is searching for a string using the grep command. She wants to restrict the search to only whole words. Which option should she use?
 - a) -w
 - b) -h
 - c) -c
 - d) -l

6. Which command performs pattern matching?
 - a) sed
 - b) syslog
 - c) grep
 - d) awk

7. Clair, a normal Linux user, is searching and replacing strings in a log file using the sed command. Which option should she use to substitute the first occurrence of the string in a line?
 - a) r
 - b) d
 - c) n
 - d) s

8. Which SELinux mode allows processes to bypass security policies?
 - a) Enforcing
 - b) Permissive
 - c) Enabled
 - d) Disabled

9. True or False? The last command displays the last 20 lines of a file by default.
☐ True
☐ False

10. True or False? The system-config-services command can be used to start and stop system services at the current runlevel.
☐ True
☐ False

LESSON 12 LAB 1

Describing Network Services

Scenario:

In this lab, you will describe network services.

1. Anne, a network administrator, is setting up a network for an insurance company that will enable the branch office in New York to communicate with its head office, which is located in another part of the same city. What type of network is Anne setting up?
 - a) LAN (Local Area Network)
 - b) MAN (Metropolitan Area Network)
 - c) CAN (City Area Network)
 - d) WAN (Wide Area Network)

2. Jane, a network administrator, wants to set up a new intranet. Which options represent the valid range of IP addresses for the intranet? Select all that apply.
 - a) 10.0.0.0 to 10.255.255.255
 - b) 127.0.0.1 to 127.255.255.255
 - c) 192.168.0.0 to 192.168.255.255
 - d) 172.16.0.0 to 172.31.255.255

3. Robert, a junior network administrator, wants to configure a wireless device in Linux. Which command will enable him to do this?
 - a) ip addr
 - b) ifconfig
 - c) iwconfig
 - d) ping

 4. Yes or No? Karl, a network administrator, is trying to connect two network types that are different using a router. Will the selected device allow him to achieve his objective?

☐ Yes

☐ No

 5. Daniel, a network engineer, is setting up a network with 200 systems and wants to assign IP addresses to the client systems automatically, and be able to access a system using its IP address or its name. Which are the two services he must enable on the client systems?
 - a) DNS
 - b) DHCP
 - c) SSH
 - d) Tunneling
-

LESSON 13 LAB 1

Describing Basic Email Services

Scenario:

In this lab, you will describe basic email services.

1. Which program is used to deliver an incoming email to the intended recipient's mailbox?
 - a) MTA
 - b) MUA
 - c) MDA
 - d) SMTP

 2. True or False? By default, the SMTP server listens to port 25 for client responses.

☐ True

☐ False
-

3. Which protocol is used to send a message from the sender's MUA to the sender's MTA?
 - a) POP3
 - b) IMAP
 - c) SMTP
 - d) POP4

4. Which file will you use to define the mapping of an IP address to the hostname?
 - a) /etc/ogc.forward file
 - b) /var/named/hosts file
 - c) /etc/resolv.conf file
 - d) /etc/hosts file

5. Which file will you use to configure sendmail?
 - a) sendmail.cf
 - b) sendmail.mc
 - c) local-host-names
 - d) domaintable

6. Which command will you use to update the aliases database?
 - a) aliases
 - b) newaliases
 - c) newaliases database filename
 - d) makemap

7. Which directive will you use to specify the location of the alias file?
 - a) alias_database
 - b) virtual_alias_maps
 - c) alias_databases
 - d) alias_maps

8. Which directive will you use to define restrictions for a sender?
 - a) smtpd_sender_restrictions
 - b) sender_restrictions
 - c) smtpd_restrictions
 - d) smtpd_sender_restriction

LESSON 14 LAB 1

Securing Linux



You can find a suggested solution for this activity in the Lesson 14 Lab 1 solution.html file in the Securing_Linux\Solution folder in the student data files.

Scenario:

An employee, Pat, asked your manager, John, to make his password more secure. John asks you to make Pat's password more secure and add additional rules to the firewall to allow Samba to communicate with the system. You need to update Pat's password and adjust the firewall rules.

1. Update the password of Pat.
 2. View the existing rules and add three new rules to the iptables firewall.
 - a. `iptables -A INPUT -p udp -s 192.168.0.0/255.255.255.0 -d 192.168.0.1/32 --dport 137 -j ACCEPT`
 - b. `iptables -A INPUT -p udp -s 192.168.0.0/255.255.255.0 -d 192.168.0.1/32 --dport 138 -j ACCEPT`
 - c. `iptables -A INPUT -p tcp -s 192.168.0.0/255.255.255.0 -d 192.168.0.1/32 --dport 139 -j ACCEPT`
-
-

LESSON 15 LAB 1

Verifying Hardware Compatibility

Scenario:

Your manager wants to place an order for new Linux systems, but is not sure about the hardware requirements. He wants you to check information available at the Red Hat site and determine which hardware will work with Red Hat Enterprise Linux.



This activity can be performed on Linux or Windows systems with Internet connectivity.

1. Log in to the GUI and launch a web browser.
 2. Access the Linux hardware compatibility article at <https://hardware.redhat.com/>.
-

3. Select the **Systems** link for **Version 5** to view the Hardware Catalog. Browse through the Hardware Catalog to check for Linux-compatible hardware.
4. Return to <https://hardware.redhat.com/> and select the **Components/ Peripherals** link for **Version 5** to view the list of components and peripherals compatible with Linux.
5. Close the web browser window.

LESSON 16 LAB 1

Troubleshooting Linux System Issues

Scenario:

As a system administrator, you may encounter many system issues that have to be rectified to restore the system or its services. So, you decide to refresh your knowledge on troubleshooting Linux systems.

1. What is the first step in troubleshooting a corrupt X Window system?
 - a) Switch to runlevel 3 to fix the issue.
 - b) Switch to runlevel 0 to fix the issue.
 - c) Switch to runlevel 6 to fix the issue.
 - d) Switch to runlevel 5 to fix the issue.
2. The _____ command is used to check the display settings.
3. In which file should the name server entry be defined to enable the domain name server to resolve the domain name to IP address?
 - a) /etc/hosts
 - b) /etc/host.conf
 - c) /etc/resolv.conf
 - d) /etc/sysconfig/network
4. Which command is used to repair a broken filesystem?
 - a) e2fsck
 - b) mkfs
 - c) fsck
 - d) dump2fs
5. You need to edit the _____ file to configure the system log information.

6. Which file is used to define the label /boot for the device /dev/sda2?
- a) e2label /dev/sda2 /boot
 - b) e2label /boot /dev/sda2
 - c) e2label /boot
 - d) e2label /dev/sda2
-
-

LESSON 17 LAB 1

Installing Linux



You can find a suggested solution for this activity in the Lesson 17 Lab 1 solution.html file in the Installing_Linux\Solution folder in the student data files.

Before You Begin:

Ensure that the five installation CDs of RHEL 5.3 are available.


Scenario:

Your manager would like you to install a fresh version of Linux on a system so that it can be duplicated and installed throughout the company. Install Linux on a system that most of the users in the company are using, to ensure that the drivers will work across the board.

-
1. Initiate the Red Hat Enterprise Linux 5 installation process for a server system.
 2. Partition the hard disk manually.
 3. Set the time zone and root password.
 4. Select the required software packages for the system.
 5. Perform installation.
 6. Configure post installation settings.
-
-

LESSON 18 LAB 1

Configuring the Linux GUI

 You can find a suggested solution for this activity in the Lesson 18 Lab 1 solution.html file in the Graphical_User_Interface\Solution folder in the student data files.

Data Files:

- A.D. MONO.ttf

Before You Begin:

If students are going to perform this lab activity immediately after Lesson 18, they need to copy the data files from the 085099Data/Graphical_Interface/ directory in the student data CD to the user's root directory. However, if they are going to perform it outside the classroom environment, they need to have the following setup:

1. A system running Red Hat Enterprise Linux 5 with the CLI components installed.
2. Data files extracted from the /085099Data/Graphical_Interface/ directory in the student data CD to the user's root directory.

Scenario:

The system allocated to a new employee has the CLI, but not the GUI. The employee asked you to configure the GUI based on the specifications listed below.

- Set the screen resolution as 1024x768 and color to millions of colors.
- Install the font A.D. MONO.ttf.
- Select the newly installed font and set the font size as 14 in KDM.

1. Enable the Linux GUI.

2. Adjust the resolution.

3. Log in as root in the KDE GUI.

4. Install the new font.

5. Configure the new font.

SOLUTIONS

Lesson 1

Activity 1-1

1. Which of these statements about open source software are true? Select all that apply.
 - ✓ a) Its source code is accessible by all.
 - ✓ b) Users have the right to modify and redistribute it.
 - c) It is always available at zero price.
 - d) It cannot be updated.
2. Which of these statements apply to Linux? Select all that apply.
 - ✓ a) Increased security
 - b) Proprietary in nature
 - ✓ c) Customizable
 - ✓ d) Easy licensing procedure
 - e) High cost
3. True or False? Software released under GPL can be modified and copyrighted by any user.
 - ___ True
 - ✓ False
4. What are the advantages of Linux? Select all that apply.
 - ✓ a) Enables software to be customized.
 - b) Comes with strong single-vendor support.
 - ✓ c) Increases the likelihood of bugs being detected because of increased numbers of programmers who can view code.
 - ✓ d) Fosters a community among users and a sense of shared responsibility for the software.
5. What are the potential disadvantages of using Linux? Select all that apply.
 - a) Licensing Linux is a difficult task and requires large amounts of money.
 - ✓ b) A limited number of mainstream applications is available.
 - ✓ c) Possible lack of comfort in believing that a single vendor can provide support.
 - d) Mainstream Linux distributions come complete with a set of games and office, network, and graphics applications.
6. True or False? There are a limited number of Linux distributions and that is why users have trouble when deciding which distribution to use.
 - ___ True

☒ False

7. True or False? Because of Linux's simple licensing terms, IT administrators do not have to spend a lot of time monitoring the number of installations or tracking licenses.

☒ True

☐ False

Activity 1-4

5. True or False? It is common practice to write a detailed report of exactly what is installed and changed on each Linux system in your environment.

☒ True

☐ False

6. What are the additional help options that may be installed on your Linux system?

☒ a) --help

b) helpme

☒ c) HOWTO

☒ d) Textinfo

7. In what formats are HOWTOs available?

☒ a) PostScript

b) Email

☒ c) PDF

☒ d) HTML

Lesson 1 Follow-up

Lesson 1 Lab 1

1. What are the benefits of releasing software under GPL?

Source code of the software will be freely available and can be modified by users. This feature enables users to customize the software to suit their requirements. GPL also prevents users from copyrighting the software after modifications, thus protecting the rights of the developer. The software will be constantly developed and improved by a community of users.

2. Identify the advantages of using open source software.

Open source software allows users to modify the source code. Users can improve the code and redistribute it freely. Moreover, the software can be used and distributed without much restriction.

3. Compare free software and proprietary software.

Free software can be freely distributed among users without any restriction. Proprietary software is bound by licensing agreements and cannot be distributed without an appropriate license. Source code of free software is freely available to users for modification and redistribution. Whereas, the source code of proprietary software is not accessible to users because it is the legal property of the owner or company.

4. List the features of Linux that make it competitive as an operating system.

Linux is available as various distributions to suit the requirements of different users. It can be downloaded free of cost or purchased at a low cost. Linux provides good security, performance, and stability.

Lesson 3

Activity 3-5

2. At which runlevel can you perform disk maintenance without damaging the disks?

- a) Runlevel 0
- ✓ b) Runlevel 1
- c) Runlevel 3
- d) Runlevel 5

3. True or False? You can run the e2fsck command to perform a disk check on a mounted filesystem.

- ___ True
- ✓ False

Lesson 4

Activity 4-8

1. True or False? When you delete a hard link, the file to which the hard link is set will also get deleted.

- ✓ True
- ___ False

3. True or False? If an executable file is located in the search path, then the user can run the file from any location.

- ✓ True
- ___ False

Lesson 5 Follow-up

Lesson 5 Lab 2

1. Which binary value allows you to assign read, write, and execute permissions to a file?
 - a) 4
 - b) 2
 - ✓ c) 7
 - d) 6
2. True or False? Only the owner of the file can change the permissions for a file or directory.
 - ___ True
 - ✓ False
3. Which option represents the default base permissions for nonexecutable files in Linux?
 - a) 777
 - b) 644
 - ✓ c) 666
 - d) 744
4. True or False? For directories created by the root user, the default permission is 644.
 - ___ True
 - ✓ False
5. True or False? The numbers given with the umask command specify the permissions that need to be cleared from the default settings.
 - ✓ True
 - ___ False
6. Chris needs to recursively change the ownership of files through a directory structure. Which option of the chown command will allow Chris to do so?
 - a) -c
 - ✓ b) -R
 - c) -v
 - d) -f
7. Which statements about sticky bits are true? Select all that apply.
 - a) Any user can delete the file or directory with a sticky bit.
 - ✓ b) A sticky bit is a permission bit that provides protection for files in a directory.
 - ✓ c) A sticky bit on a file indicates to the operating system that the file will be frequently executed.
 - d) A sticky bit closes a program or file so that it needs to be reloaded when it is invoked again.
8. True or False? ACL allows the assignment of permissions to individual users or groups even if they do not belong to the owner's group or the owning group.

- ☒ True
- ☐ False

9. True or False? By default, system processes are usually owned by the root user.

- ☒ True
- ☐ False

Lesson 6 Follow-up

Lesson 6 Lab 2

1. Which statements about CUPS are true? Select all that apply.

- ☒ a) CUPS is a systematic print management system for Linux that allows a computer to function as a print server.
- ☐ b) CUPS can process only a single data format on the same print server.
- ☒ c) CUPS is designed for scheduling print jobs, processing administrative commands, and providing printer status information to local and remote programs.
- ☒ d) A system running CUPS is a host that can initiate print jobs from client systems.

2. Which statements about print queues are true? Select all that apply.

- ☐ a) Print queues are used by the print daemon so that applications that need to use the printer have to wait for the current print job to complete before issuing the command for printing.
- ☒ b) Print queues allow multiple users to share a printer.
- ☐ c) A print queue is a storage area that sorts outgoing print jobs.
- ☒ d) Print queues contain a list of print jobs with details of the file being printed and the files yet to be printed.

3. True or False? If a printer is busy, each job is placed in a waiting line, or print queue, and stored in a temporary storage space called a print spool.

- ☒ True
- ☐ False

4. Which command allows you to start or stop a printer, enable or disable queues, manage jobs in the queue, and obtain a status report on the printers and queues?

- ☐ a) lpr
- ☐ b) lpq
- ☒ c) lpc
- ☐ d) lprm

5. You want to preview a document with double spacing using the pr command. Which option should you use?

- ☒ a) -d
- ☐ b) -m
- ☐ c) -l

d) -h

6. **True or False? The lp command sends data directly to the printer.**
☒ True
☐ False
7. **Which statements about Samba are true? Select all that apply.**
 - ✓ a) Samba is a suite of network sharing tools that help in the sharing of files and printers on a network, which consists of computers running on different operating systems.
 - ✓ b) Samba is an open source software application that provides enhanced interoperability with better performance and minimal maintenance.
 - ✓ c) Samba uses the SMB protocol to enable Linux systems to communicate with computers running on other operating systems and share network resources such as printers.
 - d) Samba is a suite of network sharing tools that help in the sharing of files and printers on a network, which consists of computers running on homogeneous operating systems.
8. **Which command allows you to use a remote printer by copying a file to the remote spool directory where it waits until the remote print server can print it?**
 - a) lprm
 - ✓ b) lpr
 - c) lpq
 - d) lpc
9. **True or False? Samba provides enhanced network security by allowing Active Directory (AD) support.**
☒ True
☐ False
10. **True or False? The /etc/hosts.lpd file lists the names of the remote computers that can use a local printer.**
☒ True
☐ False

Lesson 7

Activity 7-8

1. **Which command will you use to list the shared library files available for an executable program?**
 - a) ld /[Location of the executable file]
 - ✓ b) ldd /[Location of the executable file]
 - c) ldconfig /[Location of the executable file]
 - d) lddlibc4 /[Location of the executable file]
2. **True or False? You have added a few new library files. To update the changes to the /etc/ld.so.cache file, you need to run the ldconfig command.**

- ☒ True
- ☐ False

3. Identify the correct sequence of steps to be followed in specifying a location for the system libraries.

- 4 Save and close the file.
- 5 Log out and log in.
- 1 Access vi /etc/profile.
- 2 Type LD_LIBRARY_PATH=/usr/lib:/lib:[Location of the other library files].
- 3 Export the LD_LIBRARY_PATH variable.

Lesson 7 Follow-up

Lesson 7 Lab 2

1. Which package manager does Red Hat Linux use?
 - a) Red Hat Package Assistance
 - b) DEB
 - ☒ c) Red Hat Package Manager (RPM) or RPM Package Manager
 - d) apt-get
2. True or False? The rpm -e command is used to remove a Red Hat package.
 - ☒ True
 - ☐ False
3. True or False? Packages include all the files required to run an application.
 - ☒ True
 - ☐ False
4. True or False? To repair a package, you must first uninstall it and then reinstall it.
 - ☒ True
 - ☐ False
5. True or False? If you perform a package update and the package is not already installed on the system, it will be not be installed.
 - ☐ True
 - ☒ False
6. Janet, a junior administrator, wants to create a repository by using a local directory. But, she does not want to include all the files in the directory. Which command allows her to achieve this?
 - ☒ a) createrepo -x
 - b) createrepo -p
 - c) createrepo -h

d) createrepo -c

7. Pat, a software engineer, wants to select the checksum to be used while creating a repository. Which command does he have to use?
- a) createrepo -x
 - ✓ b) createrepo -s
 - c) createrepo -h
 - d) createrepo -c
8. True or False? Repositories contain only the source code for packages.
- ___ True
 - ✓ False
9. Robert, a system administrator, wants to view the version, dependencies, and integrity of a specific package using the dpkg command. Which option must he specify to get the desired output?
- a) -L
 - ✓ b) -p
 - c) -l
 - d) -S
10. Which statements about makefile are true?
- ✓ a) makefile contains the details of files, dependencies, and rules with which an executable application is built.
 - b) makefile is used to configure and compile driver and install application.
 - ✓ c) System built-in rules for maintaining, updating, and regenerating groups of programs are overridden by the contents of makefile.
 - d) System built-in rules for maintaining, updating, and regenerating groups of programs are not overridden by the contents of makefile.

Lesson 8

Activity 8-1

1. Which function is associated with the SCI layer of the kernel?
- a) Passing requests to device drivers
 - ✓ b) Sending service requests to the kernel
 - c) Processor time allocation for functions
 - d) Process scheduling functions
 - e) File organization
2. What are the major functions performed by the kernel? Select all that apply.
- a) Kernel initialization
 - ✓ b) Process management
 - ✓ c) Memory management

- d) Module installation
 - e) Dependency management
3. True or False? The kernel maintains a list of all the devices in the /boot directory.
- ☐ True
 - ☒ False

Lesson 8 Follow-up

Lesson 8 Lab 2

1. Which is not a core function of the Linux kernel?
 - a) Filesystem access
 - b) Resource allocation
 - c) Management of processes
 - ☒ d) Network communication
2. What function does the device management layer of the Linux kernel perform?
 - a) Enables the kernel to schedule and process function calls.
 - ☒ b) Controls interfacing between user applications and hardware devices.
 - c) Manages the computer's memory.
 - d) Allocates separate execution space on the processor for running processes.
3. What function does the SCI layer of the Linux kernel perform?
 - ☒ a) Handles function calls
 - b) Controls device access
 - c) Organizes data
 - d) Allocates execution space for processes on the processor
4. Which statements about the Linux kernel are true? Select all that apply.
 - a) In a modular kernel, all the modules are built-in.
 - ☒ b) A monolithic kernel can interact faster with devices than a modular kernel.
 - c) A monolithic kernel utilizes less RAM.
 - ☒ d) A modular kernel is also known as a micro kernel.
 - e) A monolithic kernel is also known as a dynamic kernel.
5. Anne, a Linux programmer, wants to install a specific module in the currently running kernel. Which utility should she use?
 - ☒ a) insmod
 - b) modinfo
 - c) lsmod
 - d) modprobe

6. Diana, an administrator trainee, wants to view all the current kernel parameter values in a tabular format. Which sysctl command option should she use?
 - a) -n
 - b) -P
 - c) -a
 - ✓ d) -A
7. Peter, a system programmer, wants to load a module in the initrd image before the loading of SCSI modules. Which mkinitrd command option should he use?
 - a) --builtin={module name}
 - b) --fstab={fstab}
 - ✓ c) --preload={module name}
 - d) --fstab={module name}
8. Which special device provides unlimited null characters for writing onto any program or file?
 - a) /dev/null
 - ✓ b) /dev/zero
 - c) /dev/random
 - d) /dev/null/random
9. Which special device does not provide any data to a program or file?
 - ✓ a) /dev/null
 - b) /dev/zero
 - c) /dev/zero/random
 - d) /dev/zero/urandom
10. Pam wants to view the list of devices connected to her system in text mode. Which utility should she use?
 - a) hal-devices-manager
 - ✓ b) hal-device
 - c) hal-devices
 - d) hal-device-manager

Lesson 11 Follow-up

Lesson 11 Lab 2

1. Identify the syntax of the chkconfig command.
 - ✓ a) chkconfig [option] {service name} {on|off|reset}
 - b) chkconfig [option] {on|off|reset} {service name}
 - c) chkconfig [option] {on|off|reset}
 - d) chkconfig {service name}

2. Steve, a system administrator, wants to perform automatic rotation of logs on his system. Which utility should he use?
 - a) rotate
 - ✓ b) logrotate
 - c) autologrotate
 - d) rotatelog
 - e) syslogd
3. Ruby, a network administrator, wants the syslogd utility to receive messages from a network. Which syslogd command option should she use?
 - ✓ a) -r
 - b) -d
 - c) -D
 - d) -m
4. Which utility tracks kernel messages by prioritizing them?
 - ✓ a) klogd
 - b) syslogd
 - c) syslog
 - d) lastlog
5. Jane, a Linux programmer, is searching for a string using the grep command. She wants to restrict the search to only whole words. Which option should she use?
 - ✓ a) -w
 - b) -h
 - c) -c
 - d) -l
6. Which command performs pattern matching?
 - a) sed
 - b) syslog
 - c) grep
 - ✓ d) awk
7. Clair, a normal Linux user, is searching and replacing strings in a log file using the sed command. Which option should she use to substitute the first occurrence of the string in a line?
 - a) r
 - b) d
 - c) n
 - ✓ d) s
8. Which SELinux mode allows processes to bypass security policies?
 - a) Enforcing
 - ✓ b) Permissive
 - c) Enabled
 - d) Disabled

9. True or False? The last command displays the last 20 lines of a file by default.
☐ True
☒ False
10. True or False? The system-config-services command can be used to start and stop system services at the current runlevel.
☒ True
☐ False

Lesson 12 Follow-up

Lesson 12 Lab 1

1. Anne, a network administrator, is setting up a network for an insurance company that will enable the branch office in New York to communicate with its head office, which is located in another part of the same city. What type of network is Anne setting up?
 - a) LAN (Local Area Network)
 - ☒ b) MAN (Metropolitan Area Network)
 - c) CAN (City Area Network)
 - d) WAN (Wide Area Network)
2. Jane, a network administrator, wants to set up a new intranet. Which options represent the valid range of IP addresses for the intranet? Select all that apply.
☒ a) 10.0.0.0 to 10.255.255.255
b) 127.0.0.1 to 127.255.255.255
☒ c) 192.168.0.0 to 192.168.255.255
☒ d) 172.16.0.0 to 172.31.255.255
3. Robert, a junior network administrator, wants to configure a wireless device in Linux. Which command will enable him to do this?
 - a) ip addr
 - b) ifconfig
 - ☒ c) iwconfig
 - d) ping
4. Yes or No? Karl, a network administrator, is trying to connect two network types that are different using a router. Will the selected device allow him to achieve his objective?
☐ Yes
☒ No
5. Daniel, a network engineer, is setting up a network with 200 systems and wants to assign IP addresses to the client systems automatically, and be able to access a system using its IP address or its name. Which are the two services he must enable on the client systems?
☒ a) DNS
☒ b) DHCP

- c) SSH
- d) Tunneling

Lesson 13 Follow-up

Lesson 13 Lab 1

1. Which program is used to deliver an incoming email to the intended recipient's mailbox?
 - a) MTA
 - b) MUA
 - ✓ c) MDA
 - d) SMTP
2. True or False? By default, the SMTP server listens to port 25 for client responses.
 - ✓ True
 - ___ False
3. Which protocol is used to send a message from the sender's MUA to the sender's MTA?
 - a) POP3
 - b) IMAP
 - ✓ c) SMTP
 - d) POP4
4. Which file will you use to define the mapping of an IP address to the hostname?
 - a) /etc/ogc.forward file
 - b) /var/named/hosts file
 - c) /etc/resolv.conf file
 - ✓ d) /etc/hosts file
5. Which file will you use to configure sendmail?
 - a) sendmail.cf
 - ✓ b) sendmail.mc
 - c) local-host-names
 - d) domaintable
6. Which command will you use to update the aliases database?
 - a) aliases
 - ✓ b) newaliases
 - c) newaliases database filename
 - d) makemap
7. Which directive will you use to specify the location of the alias file?
 - a) alias_database

- b) virtual_alias_maps
- c) alias_databases
- ✓ d) alias_maps

8. Which directive will you use to define restrictions for a sender?

- ✓ a) smtpd_sender_restrictions
- b) sender_restrictions
- c) smtpd_restrictions
- d) smtpd_sender_restriction

Lesson 14

Activity 14-6

1. Which operations can be performed by the nmap command? Select all that apply.

- ✓ a) Scanning entire networks for various ports and the services running on them.
- b) Returning packets to the user, if the packet header matches the expression in the query.
- c) Obtaining packet information from a query string sent to the network interface.
- ✓ d) Helping a user to get specific information about a network.

2. Which of these can be a part of an IDS? Select all that apply.

- ✓ a) Hardware sensor
- ✓ b) Intrusion detection software
- c) Log files
- ✓ d) IDS management software

3. What does Tripwire do?

- a) Protects portals, networks, and files from hackers.
- ✓ b) Compares the content of a file or directory with a database.
- c) Obtains packet information from a query string sent to the network interface.
- d) Monitors remote network connections.

4. What is Snort?

- a) A detection tool that monitors the attributes of a file such as the binary signature, size, or expected change of size.
- b) A software application that scans the ports for potential attacks.
- ✓ c) A network IDS that monitors network traffic.
- d) A tool that is used to crack system passwords.

5. Which audits the security of remote hosts and services running on a network?

- a) Portsentry
- ✓ b) Nessus

- c) Tripwire
- d) Snort

6. What does portsentry do when a port attack is detected?

When a port attack is detected, portsentry generates a log entry that contains the details of the hostname, the time of attack, the attacking host's IP address, and the TCP or the UDP port.

Lesson 15

Activity 15-2

1. Which of these statements are true? Select all that apply.
 - a) USB is an IEEE 1394-standard, high-speed serial bus.
 - ✓ b) A loopback device allows you to mount filesystem images, such as ISO, on the hard disk.
 - ✓ c) FireWire is ideal to connect a digital video camera to a system.
 - d) The PCMCIA was formerly known as the PC Card.
 - e) The cardmgr utility is used to monitor and control the state of PCMCIA sockets.
2. Which is the earliest kernel that supported USB?
 - ✓ a) 2.2.18
 - b) 2.4.16
 - c) 2.6.22
 - d) 2.2.13
3. True or False? USB device information is located in the /proc/usb directory.
 - ___ True
 - ✓ False

Lesson 16

Activity 16-4

1. In which file will you change the LCD monitor parameters such as DefaultDepth, Viewport, and Depth?
 - a) /etc/x11Config
 - b) /etc/XF86
 - c) /X11/XF86Config
 - ✓ d) /etc/X11/xorg.conf

2. One of the LCD monitors is not displaying any output. What could be the problem? Select all that apply.
 - ✓ a) The LCD panel is not connected properly to the system.
 - ✓ b) The VGA card module is not configured properly.
 - c) Serial port settings are not configured properly.
 - ✓ d) Monitor parameters, such as DefaultDepth, Viewport, and Depth, are not configured properly.
3. True or False? In the `/etc/X11/xorg.conf` file, the Screen section contains parameters of the VGA card module for an LCD monitor.
 - ✓ True
 - ___ False
4. In one of the terminals, users are not able to listen to the audio associated with the animation. What will be your first step to troubleshoot the issue?
 - a) Verify that the sound card is detected while booting.
 - b) Verify that the sound card module is loaded.
 - c) Contact the hardware engineer to solve the issue.
 - ✓ d) Verify that the speaker is connected, switched on, and working properly.
5. Which command will you use to verify serial port settings?
 - a) `setserial -q`
 - b) `setserial -v`
 - ✓ c) `setserial -a`
 - d) `setserial -z`

Activity 16-5

1. One of your network users is unable to connect to the FTP server, which is located on a different network. The error message indicates that the other network is unreachable. You verified that the network cable is intact and that the FTP server is up. What could be the probable cause of the error? Select all that apply.
 - ✓ a) The network service is not up.
 - b) The `resolv.conf` file does not contain entries for the name server.
 - ✓ c) Network parameters, such as the IP address, the subnet mask, or the default gateway, are not set correctly.
 - d) The firewall is disabled.
2. You verified that the network service is running and that the network parameters are properly set. However, the user is still unable to connect to the network. What will be your first step to troubleshoot the network issue?
 - a) Verify that the hostname is set.
 - ✓ b) Verify that the DNS entries are correct.
 - c) Verify that IP forwarding is enabled.
 - d) Verify that the ports of the service you are trying to access are open at the destination host.
3. True or False? To set the hostname permanently, you need to modify the `/etc/sysconfig/network` file.

- ☒ True
☐ False

Lesson 16 Follow-up

Lesson 16 Lab 1

1. What is the first step in troubleshooting a corrupt X Window system?
☒ a) Switch to runlevel 3 to fix the issue.
b) Switch to runlevel 0 to fix the issue.
c) Switch to runlevel 6 to fix the issue.
d) Switch to runlevel 5 to fix the issue.
2. The system-config-display command is used to check the display settings.
3. In which file should the name server entry be defined to enable the domain name server to resolve the domain name to IP address?
a) /etc/hosts
b) /etc/host.conf
☒ c) /etc/resolv.conf
d) /etc/sysconfig/network
4. Which command is used to repair a broken filesystem?
a) e2fsck
b) mkfs
☒ c) fsck
d) dump2fs
5. You need to edit the /etc/syslog.conf file to configure the system log information.
6. Which file is used to define the label /boot for the device /dev/sda2?
☒ a) e2label /dev/sda2 /boot
b) e2label /boot /dev/sda2
c) e2label /boot
d) e2label /dev/sda2

Lesson 17

Activity 17-1

1. What is the default boot loader in new versions of Red Hat Enterprise Linux?
 - a) LILO
 - ✓ b) GRUB
 - c) System Commander
2. True or False? FIPS is used to resize FAT partitions.
 - ✓ True
 - ___ False
3. When is it the best time to gather information about your Linux system?
 - a) Just after installing Linux.
 - b) During the Linux installation.
 - ✓ c) Before installing Linux.
 - d) You do not have to gather system information.

Activity 17-2

1. What enables you to choose the operating system to load from the hard disk?
 - a) The boot loader
 - ✓ b) MBR
 - c) The number of tracks on the hard disk
 - d) BIOS
2. What is true of MBR? Select all that apply.
 - ✓ a) MBR contains the partition tables.
 - b) MBR contains a number of sectors.
 - ✓ c) MBR contains the code to load the operating system into memory.
 - d) MBR determines the boot device settings.
 - ✓ e) MBR determines the currently active partition.
3. True or False? The boot loader installer contains a kernel loader.
 - ___ True
 - ✓ False

INDEX

/usr subdirectories, 96
\$HISTFILESIZE, 350

A

Access Control List
 See: ACL
access control types, 450
accessibility based themes, 711
accessibility features, 710
accessibility options, 710
ACL, 220
Address Resolution Protocol
 See: ARP
advanced permission commands, 220
algorithms, 555
alien, 280
Anaconda installer, 647
archiving, 174
argument, 14
ARP, 635
authentication methods, 553
autoconf, 285
automatic rotation, 437
average time, 415
 Also See: true time

B

background processes, 382
backup strategy guidelines, 179
Bash shell, 330
Bash shell functions, 331
basic architecture of USB driver
 host computer, 600
 host controller hardware layer, 601
 physical bus, 601
 upper software layer, 600
 USB devices, 601
basic filesystem commands, 101

Basic Input/Output System
 See: BIOS
Beagle, 150
binaries, 108
BIND attack, 636
biometric authentication, 554
BIOS, 650
block special files, 94
boot disks, 617
boot loader, 42
boot loaders, 656
 components, 656
 types, 657
boot managers, 656
 Also See: boot loaders
boot process, 658
booting devices, 652
Bourne-Again SHell
 See: Bash shell
broadcast addresses, 464
browser mode, 97
built-in help options, 32

C

cat command options, 23
CDPATH, 348
cells, 472
central network log server, 436
chains, 578
Challenge Handshake Authentication Protocol
 See: CHAP
CHAP, 554
character special files, 94
check for dependency, 278
child process, 351
chmod command modes, 203
chmod command options, 203
chroot mode, 614
classless addressing, 464

- CLI, 10
- clock drift, 419
- CMOS, 651
- Command Line Interface
 - See:* CLI
- command line interpreter, 10
- command prompt, 10
- command substitution, 363
- commands
 - :help, 134
 - :q, 134
 - #!/bin/bash, 341
 - \$SHELL, 13
 - alias, 349
 - apropos, 31
 - apt-get, 279
 - aptitude, 280
 - aspell, 139
 - at, 410
 - awk, 442
 - bash, 12
 - cal, 16
 - cardmgr, 598
 - cat, 23
 - chatr, 217
 - chkconfig, 430
 - chmod, 202, 351
 - chown, 68, 213
 - cpio, 175
 - createrepo, 270
 - cs, 12
 - date, 15
 - dd, 175, 618
 - debugfs, 120
 - df, 594
 - dhcpcclient, 475
 - diff, 137
 - dig, 496
 - du, 594
 - dump, 176
 - dumpe2fs, 119
 - e2fsck, 118
 - e2label, 77
 - echo, 13, 21, 347
 - exit, 12
 - export, 346
 - fdisk, 81, 648
 - file, 94
 - find, 150
 - finger, 53
 - for, 371
 - free, 322
 - fsck, 117
 - gedit {file name}, 60
 - GNU parted, 87
 - gpg, 557
 - grep, 148, 440
 - groupadd, 53
 - groupdel, 67
 - groupmod, 67
 - gzip, 177
 - head, 13
 - history, 333
 - host, 497
 - hostname, 19
 - id, 52, 567
 - if, 370
 - if...else, 370
 - ifconfig, 470
 - ifdown, 471
 - ifup, 471
 - inetd, 432
 - ip, 487
 - iwconfig, 471
 - jobs, 383
 - last, 21
 - lastlog, 440
 - ln, 168
 - locate, 147
 - logrotate, 408, 437
 - logwatch, 409
 - lpc, 235
 - lpd, 40
 - lpr, 235
 - ls, 59
 - ls -a, 59
 - lsattr, 218
 - m4, 528
 - make, 557
 - man, 30
 - md5sum, 556
 - mkdir, 68
 - mke2fs, 85
 - mkfs, 84
 - mkinitrd, 308
 - mknod, 315
 - mkswap, 110
 - more, 13

- more /etc/passwd, 13
- mount, 107
- netstat, 486
- nice, 396
- nohup, 403
- nslookup, 498
- ntpdate, 423
- openssl, 557
- partprobe, 86
- passwd, 50
- passwd -l, 67
- patch, 138
- pccardctl, 599
- ping, 461
- pmap, 323
- pr, 235
- printconf, 240
- printtool, 240
- ps, 388
- pstree, 391
- pump, 475
- pwd, 98
- quotacheck, 605
- rdesktop, 514
- rdev, 617
- read, 359
- renice, 397
- repomd, 270
- restore, 180
- rm, 566
- route, 483
- rpm, 559
- rpm -Fvh *.rpm, 267
- rpm2cpio, 260
- sar, 324
- scp, 509
- sed, 444
- sfdisk, 86
- sftp, 509
- shasum, 556
- shutdown, 42
- sleep, 22
- slocate, 148
- ssh-keygen, 506
- startx, 687
- su, 566
- sudo, 567
- swapoff, 110
- swapon, 110
- switchdesk, 699
- sysctl, 304
- syslogd, 437
- system-config-date, 419
- system-config-services, 431
- tail, 13, 441
- tar, 176
- tee, 363
- test, 342
- tmpwatch, 408
- top, 395
- tr, 139
- traceroute, 485
- tune2fs, 118
- umask, 209
- umount, 107
- uniq, 139
- unset, 62
- unzip, 178
- uptime, 17
- useradd, 49
- userdel, 65
- usermod, 66
- vim, 132
- vimdiff, 138
- vimtutor, 134
- vmstat, 323
- vncserver, 512
- vncviewer, 513
- w, 20
- wc, 138
- whatis, 31
- whereis, 148
- which, 24, 61
- while, 372
- who, 18
- whoami, 19
- xargs, 362
- xauth, 687
- xinetd, 432
- xinit, 687
- xvidtune, 691
- yum, 559
- Common UNIX Printing System
 - See:* CUPS
- Complementary Metal Oxide Semiconductor
 - See:* CMOS
- configure, 278

- console, 13
 - Also See:* terminal
- control statements, 367
- copyleft, 4
- core system variables, 616
- counts, 136
- cron jobs, 407
- crontab, 406
- cryptographic hashes, 556
- CUPS, 228
- cylinder, 86
- D**
- daemons, 40, 382
 - anacron, 412
 - cron, 406
 - hald, 318
 - httpd, 546
 - klogd, 438
 - logging service, 435
 - mysqld, 189
 - ntpd, 416
 - slapd, 473
 - squid, 546
 - xinetd, 543
- Data Encryption Standard
 - See:* DES
- databases, 186
- datagrams, 482
- date Command characters, 16
- date/time format, 420
- DBus, 319
- DEB tools, 278
- Debian installation process, 278
- Debian package management commands, 279
- default environment variables, 349
- default gateway addresses, 485
- default gateways, 485
- default permissions, 209
- default user accounts, 50
- DES, 555
- device drivers, 313
- device nodes, 314
- device tree, 313
- DHCP, 491
- DHCP components, 491
- DHCP process, 493
- digital certificates types
 - Certificate Authority, 559
 - Self-signed, 559
- directories
 - /boot/grub, 663
 - /etc/cups, 245
 - /etc/init.d, 429
 - /etc/localtime, 422
 - /etc/ntp, 416
 - /etc/sysconfig, 431
 - /etc/xinetd.d, 545
 - /lib/modules, 299
 - /proc, 303
 - /sys, 313
 - /usr/lib/rpm/*, 258
 - /usr/share/doc, 32
 - /usr/share/zoneinfo/, 422
 - /var/lib/dpkg/*, 280
 - RPMS, 258
 - skel, 59
- directory
 - current working, 98
 - home, 97
 - parent, 99
- directory service, 473
- disk image, 107
 - Also See:* ISO image
- disk quotas, 604
- display managers, 696
 - GDM, 697
 - KDM, 697
- DNS, 493
- DNS resource records, 499
- documentation, 679
- domain name resolution process, 496
- Domain Name System
 - See:* DNS
- domain names, 494
- domains, 494
- drivers, 286
- Dynamic Host Control Protocol
 - See:* DHCP
- E**
- editing operators, 136
- electronic mailing process, 530
- ELILO, 657
- encryption, 555
 - asymmetric, 557
 - symmetric, 557
- encryption solutions, 555

- 3DES, 555
- Blowfish, 555
- MD5, 555
- entropy, 315
- environment configuration problems, 615
- environment files, 565
- environment variable
 - PATH, 351
- environment variables, 348
- execute mode commands, 134
- expressions, 367

F

- fdisk utility options, 82
- FHS, 94
- fields, 186
- file archiving utilities, 178
- file browsers, 96
- file compression utilities, 178
- file naming conventions, 96
- file owner, 202
- File Transfer Protocol
 - See:* FTP
- files
 - .rhosts, 509
 - .shosts, 509
 - ~/bash_profile, 59
 - /etc/crontab, 410
 - /etc/group, 54
 - /etc/hosts.equiv, 244
 - /etc/hosts.lpd, 244
 - /etc/issue, 180
 - /etc/issue.net, 180
 - /etc/login.defs, 565
 - /etc/passwd, 51
 - /etc/shadow, 52
 - /etc/skel, 59
 - /etc/ssh/ssh_config, 507
 - /etc/syslog.conf, 438
 - /etc/timezone, 422
 - /etc/xinetd.conf, 544
 - /proc/modules, 299
 - /proc/version, 302
 - /var/log/lastlog, 440
 - /var/log/messages, 438
 - apt.conf, 280
 - boot.iso, 617
 - diskboot.img, 617
 - fstab, 83

- grub.conf, 663
- inittab, 428
- known_hosts, 508, 553
- libwrap.so, 545
- log, 435
- makefile, 284
- menu.lst, 663
- modprobe.conf, 301
- named.conf, 499
- NTP drift, 416
- ntp.conf, 416
- printers.conf, 245
- sysctl.conf, 304
- tw.cfg, 586
- xorg.config, 692
- Filesystem Hierarchy Standard
 - See:* FHS
- filesystem integrity, 117
- filesystem labels, 77
- filesystem maintenance tasks, 116
- filesystem management tasks, 106
- filesystem types, 78
- filesystems, 77
- filters, 161
- find command conditions, 152
- FIPS, 650
- firewalls, 575
 - hardware, 576
 - software, 576
- FireWire, 601
- First nondestructive Interactive Partition Splitting
 - program
 - See:* FIPS
- font path, 686
- foreground processes, 381
- Free Software Foundation
 - See:* FSF
- FSF, 3
- FTP, 460
- Fully Qualified Domain Name
 - See:* FQDN
- functions, 368

G

- gateways, 485
- GCC, 302
- General Public License
 - See:* GPL
- global user profiles, 59

- globbing, 332
- GMT, 416
- GNOME desktop environment, 697
- GNOME On-Screen Keyboard
 - See:* GOK
- GNOME search tool, 149
- GNOME system monitor, 325, 397
- GNU Compiler Collection, 302
 - Also See:* GCC
- GNU project, 3
- GOK, 710
- GPL, 4
- GRand Unified Bootloader
 - See:* GRUB
- Graphical User Interface
 - See:* GUI
- Greenwich Mean Time
 - See:* GMT
- group database, 54
- group management, 67
- groups, 53
- GRUB, 662
 - commands, 664
 - menu-specific commands, 665
- GUI, 10

H

- HAL, 318
 - utilities, 318
- hardware
 - components, 592
 - resources, 592
- Hardware Abstraction Layer
 - See:* HAL
- hardware communication channels, 317
 - Direct Memory Address (DMA), 318
 - Input/Output (I/O) Addresses, 317
 - Interrupt ReQuests (IRQ), 317
- hardware compatibility, 644
- hardware device types, 314
- hardware problems, 628
- HCI, 601
- honeypot, 637
- Host Controller Interface
 - See:* HCI
- HTTP, 460
- HyperText Transfer Protocol
 - See:* HTTP

I

- IANA, 467
- ICMP, 461
- IDS, 585
 - active, 585
 - passive, 585
- ifconfig command options, 471
- IMAP, 526
- immutable flag, 219
- index node, 167
 - Also See:* inode
- index node table, 167
- init, 40
- init process, 381
- initrd, 307
- initrd image, 308
- inodes, 167
- input and output redirection, 140
- Internet Assigned Numbers Authority
 - See:* IANA
- Internet Control Message Protocol
 - See:* ICMP
- Internet Message Access Protocol
 - See:* IMAP
- Intrusion Detection System
 - See:* IDS
- IP address classes
 - Class A, 464
 - Class B, 464
 - Class C, 464
- IP addresses, 461
- IP addresses allocation, 492
- IP classes, 462
- IP filtering, 578
- IP Next Generation
 - See:* IPng
- IP spoofing, 636
- IP Version 4
 - See:* IPv4
- IP Version 6
 - See:* IPv6
- ipchains, 578
- IPng, 461
- iptables, 578
- IPv4, 461
- IPv6, 461
- ISO image, 107
- iwconfig command options, 471

J

job control tools, 385

jobs

 delayed, 402

 detached, 403

jobs table, 383

joins, 191

 inner, 191

 outer, 191

journaling filesystems, 117

K

Kat, 150

KDE desktop environment, 697

Kerberos, 554

kernel, 5, 295

 layers, 295

 modular, 297

 monolithic, 297

 versions and modules, 295

kernel configuration

 persistent, 302

 transactional, 302

kernel module, 298

kernel module utilities, 299

kernel options, 302

kernel state monitoring utilities, 321

key files, 507

keyboard accessibility options, 710

keys, 552

 private, 553

 public, 553

kill commands, 393

L

LAN, 459

LDAP, 473

LDAP process, 474

leap seconds, 417

LED, 470

libwrap.so.0, 561

Lightweight Directory Access Protocol

See: LDAP

links

 hard, 169

 symbolic, 169

Linux, 5

 benefits, 7

 uses, 6

Linux distributions, 7

Linux documentation, 29

Linux installation methods, 646

Linux kernel, 295

Linux rescue environment, 613

Linux User Groups

See: LUGs

LMTP, 527

LNx-BBCs, 627

load average, 321

Local Area Network

See: LAN

Local Mail Transport Protocol

See: LMTP

local storage devices, 116

locale settings, 417

log file analysis, 439

logger, 438

Logical Volume Manager

See: LVM

login levels, 565

loopback device, 601

loops, 370

LUGs, 33

LVM, 648

M

MAC address, 469

Mail Delivery Agents

See: MDAs

mail forwarding, 530

mail protocols, 524

mail queues, 526

Mail Retrieval Agents

See: MRAs

Mail Transfer Agents

See: MTAs

Mail User Agents

See: MUAs

major number, 314

makefile commands, 284

MAN, 459

man command options, 30

manual pages, 30

Master Boot Record

See: MBR

MBR, 660

MDAs, 529

Media Access Control (MAC) address, 469
 Also See: physical address
 memory monitoring utilities, 322
 memory usage, 569
 message digests, 555
 message of the day
 See: motd
 Metropolitan Area Network
 See: MAN
 minor number, 314
 modprobe, 300
 motd, 180
 motions, 135
 mount command options, 108
 mount points, 107
 MRAs, 530
 MTAs, 527
 types, 527
 MUAs, 529
 multiple SSH connections, 509
 multitasking, 383
 MySQL, 187
 MySQL commands, 189
 MySQL configuration file, 188

N
 Nessus, 588
 netfilter, 576
 Network Interface Card
 See: NIC
 network interfaces, 468
 physical, 468
 virtual, 468
 network issues, 634
 network monitoring utilities, 584
 network protocols, 460
 types, 460
 network security problems
 symptoms of, 635
 network security vulnerabilities, 636
 Network Time Protocol
 See: NTP
 network troubleshooting utilities, 634
 networks, 458
 types, 459
 NIC, 468
 characteristics, 469
 nice value, 396
 NTP, 415

O
 online help, 33
 open source software, 2
 OpenSSH, 506

P
 package dependencies, 256
 package integrity, 559
 package managers, 255
 package verification error codes, 264
 packages, 254
 packet filtering, 576
 packet-switching technology, 482
 packets, 482
 Page Description Language
 See: PDL
 PAP, 554
 Parent Process ID, 390
 Also See: PPID
 partition management, 86
 partition types, 81
 partition utilities, 648
 partitionless installation, 650
 partitions, 80
 partprobe program, 88
 Password Authentication Protocol
 See: PAP
 password policies, 568
 passwords, 50
 PATH variable, 24
 paths, 99
 absolute, 100
 relative, 100
 PC Card, 597
 PDL, 227
 Perl, 436
 permission levels, 202
 permissions, 200
 physical address, 469
 PID, 381
 ping command options, 475
 pipe, 361
 PKC, 505
 POP3, 526
 port forwarding, 511
 port ranges, 467
 ports, 465
 portsentry, 587
 POST, 650

Post Office Protocol version 3
See: POP3
 PostScript®, 227
 Power-On Self Test
See: POST
 PPID, 390
 pr command options, 236
 Practical Extraction and Reporting Language
See: Perl
 print process, 228
 print queues, 229
 print servers, 243
 printer commands, 234
 printer software, 226
 private networks, 462
 PRNG, 556
 Process ID, 381
Also See: PID
 process identification commands, 392
 process monitoring, 324
 process states, 395
 process table, 387
 processes, 381
 child, 390
 parent, 390
 profile file, 59
 program, 382
 programming constructs, 368
 proxy server implementation, 577
 proxy servers, 510
 ps command options, 389
 Pseudo Random Number Generation
See: PRNG
 Public Key Cryptography
See: PKC

Q

quota management commands, 605
 quota report contents
 grace period, 605
 hard limit, 605
 soft limit, 605
 quota reports, 605
 quota reports generation commands, 606

R

RADIUS, 560
 RAID, 648
 ramdisk word, 617

ramdisks, 617
 random number generation, 556
 RDBMS, 187
 rdesktop command options, 514
 Real Time Clock
See: RTC
 redirectors, 360
 Redundant Array of Independent Disks
See: RAID
 regular expressions, 157
 Relational Database Management System, 187
Also See: RDBMS
 relational databases, 187
 Remote Authentication Dial In User Service
See: RADIUS
 Remote Monitoring
See: RMON
 remote printer permissions, 244
 remote printing, 243
 remote X sessions, 687
 commands, 688
 removable hardware types, 597
 repair filesystems, 118
 repartitioning
 destructive, 649
 nondestructive, 649
 repositories, 270
 local or private, 270
 online, 270
 rescue environment utilities, 614
 resolver files, 498
 RMON, 515
 rogue public keys, 559
 root disks, 618
 root user, 97
 routers, 481
 routing, 481
 routing tables, 483
 RPM, 257
 commands, 258
 components, 258
 queries, 259
 verification, 263
 RPM Package Manager
 RPM, 257
 RTC, 419
 RTS, 472
 runlevel, 40

S

- Samba, 244
- SASL, 473
- SCSI, 592
- SCSI IDs, 593
- SCSI types, 593
- search paths, 351
- sectors, 660
- Secure Shell
 - See:* SSH
- Secure Socket Layer
 - See:* SSL
- security policies, 452
- Security-Enhanced Linux
 - See:* SELinux
- SELinux, 451
- SELinux modes, 452
- server keys, 508
- service and application access controls, 546
- services, 39
- Set Group ID, 217
 - Also See:* SGID
- Set User ID, 217
 - Also See:* SUID
- SGID, 217
- shadow password file, 569
- shadow passwords, 52
- shared libraries, 289
- shell commands, 13
- shell scripts, 340
- shell spawning, 351
- shells, 11
- signals, 393
- Simple Authentication and Security Layer
 - See:* SASL
- Simple Mail Transfer Protocol
 - See:* SMTP
- Simple Network Management Protocol
 - See:* SNMP
- single-user mode, 616
- Small Computer Systems Interface
 - See:* SCSI
- SMTP, 525
- SNMP, 514
- snort, 587
- snort command options, 587
- software acquisition, 8
- spatial mode, 97
- special devices, 315
- special permissions, 217
- spool, 229
- spooling, 229
- SSH, 505
- SSH protocol versions, 509
- ssh-agent, 508
- SSL, 473
- standard directories, 95
- standard error, 360
 - Also See:* STDERR
- standard groups, 53
- standard input, 359
 - Also See:* STDIN
- standard output, 359
 - Also See:* STDOUT
- status indicator lights
 - activity light, 470
 - link light, 470
 - speed light, 470
- STDERR, 360
- STDIN, 359
- STDOUT, 359
- sticky bits, 219
- subdomains, 495
- subnet masks, 463
- subnets, 472
- SUID, 217
- SUID scripts, 351
- superblocks, 659
- swap files, 109
- swap partitions, 109
- swap space, 109
- swap space types, 109
- switch modes, 133
- system initialization, 428
- system load, 322
- system logs, 435
- system security monitoring tools, 635
- system time, 419

T

- tab completion, 333
- tarballs, 285
- TCP wrappers, 561
- TCP/IP, 460
- Telnet, 543
- terminal, 13
- test constructs, 368
- text editor, 131

- text editors list, 132
- text streams, 162
- textutil commands, 164
- Transmission Control Protocol/Internet Protocol
 - See:* TCP/IP
- Tripwire, 585
- Tripwire database, 586
- troubleshooting strategies, 612
- troubleshooting tools, 627
- true time, 415
- tunneling, 510

- U**
- udev, 312
- UDP, 461
- UID, 48
- Universal Serial Bus
 - See:* USB
- Universal Time Coordinated
 - See:* UTC
- Unix, 3
- UPG, 54
- Upgrade/Freshen Packages, 266
- USB, 600
- USB devices, 600
- user accounts, 48
- User Datagram Protocol
 - See:* UDP
- User ID
 - See:* UID
- User Private Group
 - See:* UPG
- user profiles, 58
- user-level security
 - ways to improve, 569
- UTC, 416
- v, 278

- V**
- variables, 346, 369
- verbose, 84
- Vim help options, 134
- Vim modes, 133
- virtual desktops, 679
- Virtual Network Computing
 - See:* VNC
- VNC, 511

- W**
- WAN, 459
- Wide Area Network
 - See:* WAN
- wildcards, 331
- window environment, 704
- window managers, 696
 - Also See:* display managers

- X**
- X, 678
 - Also See:* X Windows
- X clients, 686
- X Display Manager
 - See:* xdm
- X font servers
 - See:* Xfs
- X forwarding, 510
- X protocol, 685
- X servers, 685
- X Windows, 678
- X-stations, 688
- X.Org, 684
- X11, 678
 - Also See:* X Windows
- xdm, 697
- Xfs, 686
- xfstools, 120
- xinetd access controls, 546
- XOrg runlevels, 687
- XTerm, 704

- Y**
- Yellow dog Updater, Modified
 - See:* YUM
- YUM, 274
 - commands, 275

- Z**
- zero-filled files, 618
- zones, 495
 - forward, 495
 - reverse, 496

